Journal of Advanced Computer Science and Technology, 3 (2) (2014) 143-153
©Science Publishing Corporation
www.sciencepubco.com/index.php/JACST
doi: 10.14419/jacst.v3i2.3321
Research Paper

Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition

Anass RGHIOUI*, Anass KHANNOUS, Mohammed BOUHORMA

Laboratory of Informatics, Systems and Telecommunications
Faculty of Science and Technology of Tangier
Abdelmalek Essaadi University, Morocco
**Corresponding author E-mail:: rghioui.anass-etu@uae.ac.ma*

Abstract

RPL (Routing Protocol for Low-power and lossy networks) is a specific routing protocol designed to optimize 6LoWPAN (IPv6 over Low power Wireless Personal Area Network) operation. As 6LoWPAN suffers from resource constraints on battery, processor, memory and bandwidth, it affects the performance of the RPL protocol. From security point of view, this will make RPL vulnerable to several threats directly or indirectly. Thus, cryptographic systems are not sufficient to protect the RPL from internal attacks; a compromised node from the network may cause undesired operation without being detected by these systems. An intrusion detection system (IDS) should be used, but it is not easy given the nature of 6LoWPAN; on a side its resource constraints, and on the other side its opening to the outside world through the Internet.

In this paper we focus on denial of service (DoS) attacks, we determine the elements to be taken into account in selecting a compatible IDS and we give some solutions that we consider effective and valid for 6LoWPAN-RPL based networks.

Keywords: *RPL, ROLL, 6LoWPAN, IDS, DoS, Network security.*

1. Introduction

The Internet of Things (IoT) main concept aim to interconnect heterogeneous objects localized separately in different places, using standard internet protocols. The idea is create an autonomous world using smart objects that have the ability to exchange information and make decisions [1]. Connected objects will give to users the possibility of monitoring and tracking anything remotely and in a real time [2], [3]. Many real-life applications can benefit from this concept like healthcare, transportation, environment, cities management, etc.

To make the concept of IoT real, IETF (Internet Engineering Task Force) created the 6LoWPAN [4], [5]. 6LoWPAN is the acronym of IPv6 over Low power Wireless Personal Area Network, i.e. making low power devices like IEEE 802.15.4-based wireless nodes [6] used in personal area networks like WSN (Wireless Sensor Network) able to connect to the internet having an IPv6 address.

6LoWPAN introduced new concepts and measures that are not dealt by other standard routing protocols in wireless networks, such as AODV, OLSR, DYMO, DSR, etc. Especially shared characteristics between all LoWPANs

(Low power Wireless Personal Area Networks) like limited processing power, very dynamic topologies, node mobility, link failures, high loss rates, low data rates and instability. To deal with this challenge, IETF create a new protocol compatible to LoWPAN networks under the name of RPL (Routing Protocol for Low-power and lossy network) [7]. RPL deal with limited memory resources of low-power nodes, link failures, traffic control cost, and its takes into consideration node and link properties when choosing routes.

Having a resource-constrained network implementing new protocols and connected to the Internet; makes it security a big challenge that must be addressed carefully [8]. Even if it implement known protocols and standards like IPv6 and 802.15.4, which possess many security solutions; it does not solve the problem. On the contrary, it aggravates the situation. Combining between two different networks; i.e. IP and 802.15.4 networks, means that we will combine their issues too. Their solution are not compatible to 6LoWPAN networks. IPv6 security protocols are very heavy and consume a lot of energy, and 802.15.4 security solutions does not deal with IP communications. Moreover, the new routing protocol RPL was designed without security metrics, knowing that the majority of attacks aim to perturb network routing to cause its dysfunction, totally or partially [9].

Several attacks can target 6LoWPAN, among these threats are whose called denial of service (DoS) attacks [10]. This type target the availability of the network, it aims to make it unavailable for an indefinite period. The main goal of such an attack is to damage the network and affect its performance. Its purpose is not to eavesdrop or alter data. A cryptography system cannot alone defend against DoS attack, even from an insider malicious node or from the internet side. An adversary may compromise some nodes, retrieve cryptographic materiel from them and modify their system to use them for malicious purposes. That why an intrusion detection system (IDS) should be used because it monitors nodes behavior and gives alerts in case of a doubt of an attack.

6LoWPAN-RPL security problems are multiple and varied against each layer [11], differs from passive and active attacks, even from the inside or the outside. This paper provides a state-of-the-art of the attacks targeting the availability of 6LoWPAN aiming to disrupt its routing protocol RPL, with the concentration on the denial of service attacks, their types and their damages. Moreover, this paper provides security solutions requirements to deal with DoS attacks, focusing on the IDS approach, by giving recommendations and directions of our vision of the IDS design that will be compatible to 6LoWPAN-RPL networks.

The structure of the paper is as follows: Section gives an overview of 6LoWPAN network and its underlying RPL, Section 3 gives more detail on RPL operation, Section 4 discusses denial of service issues and attacks, Section 5 reviews the main countermeasures to secure network routing, Section 6 focus on the IDS approach and techniques and Section 7 concludes the paper.

2. Overview

2.1. Internet of Things

Internet of Things is a concept that aims to extend the internet to the real world by associating labels bearing codes, RFID tags or URLs to objects or places, making them available and accessible from anywhere and anytime. Many technologies must be used and integrated to achieve this goal. Devices are different, some of them, like Wireless Sensor Network are resource-constrained, they are not compatible with internet communication protocols. These protocols must be adapted or new ones must be developed.

Applications domains include: waste management, urban planning, environmental sensing, social interaction gadgets, sustainable urban environment, continuous care, emergency response, intelligent shopping, smart product management, smart meters, home automation and smart events [12].

2.2. 6LoWPAN

To integrate this kind of network to the internet, An IETF workgroup under the name of 6LoWPAN (IPv6 over LoWPAN) was created to find an appropriate solution. The IETF 6LoWPAN WG introduced the use of IPv6 in the IEEE 802.15.4-based devices within 2 RFCs 4919 [4] and 4944 [5]. IEEE 802.15.4 [6] is a standard that defines the MAC and Physical layers protocols of low power and resource-constrained wireless devices. 6LoWPAN concept based on the combination between IPv6 network and the IEEE 802.15.4 network, two totally different networks. Their major difference is that the IPv6 network layer packet measures 1,280 bytes, where 802.15.4 data link layer (MAC layer) supports only packet of 127 bytes maximum.

The IETF WG proposed as a solution to add an adaptation layer between the network layer (IPv6) and the data link layer (802.15.4 MAC) to optimize IPv6 packets by the fragmentation and assembly mechanism.

6LoWPAN network consists of one or more stub networks connected to the internet through the Border Router (Fig. 1). This latter, called also Edge Router, routes traffic in and out of the LoWPAN, which is the collection of 6LoWPAN nodes sharing the same address prefix IPv6, ie the first 64 bits, it is used with IID (Interface Identifier) to form the IP address. This address is formed using the SSA (Stateless Address Autoconfiguration) in the starting phase of the network construction: the bootstrapping. This phase is managed by the data link layer, which allows the establishment of first communications between nodes to configure channel, security keys and addressing.

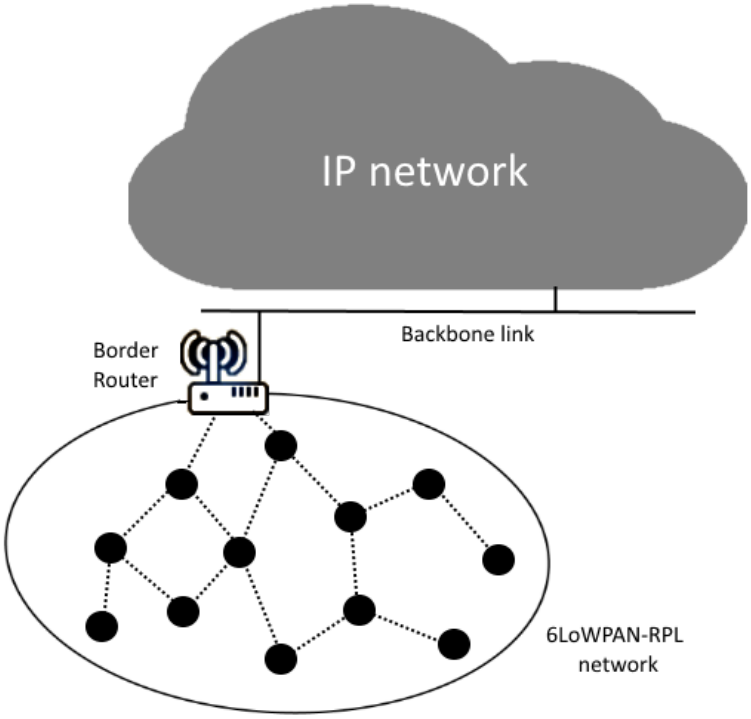

Fig. 1: 6LoWPAN-RPL network architecture

After the bootstrapping phase, and once the data link layer is functional, 6LoWPAN Neighbor Discovery protocol [13] that was chosen instead of the Neighbor Discovery protocol [14] because of its incompatibility with the low-power wireless networks - is used to start the construction of the entire network through some messages exchanged between nodes that allow hosts, routers and Border Router autoconfiguration.

2.3. RPL

Regarding routing, 6LoWPAN network has introduced new concepts and measures that are not dealt by other standard routing protocols in wireless networks, such as AODV, OLSR, DYMO, DSR, etc. Studies [15][17] showed that they are not well suited for LoWPAN networks as they consume more energy, they do not handle failure cases to establish a connection and they does not take on consideration nodes and links properties in establishing routes. Routers in LoWPAN networks uses only one wireless interface to forward packets from one node to its neighbor node, it ensures full connectivity between network nodes in forwarding packets via the same link through multi-hops toward nodes that are not accessible through a single wireless transmission.

Routing protocols in LoWPAN networks have many constraints such as minimizing energy consumption, support nodes sleep cycles, consider the quality of service, support different types of addressing (unicast, multicast, anycast), support mobility, etc. All of that must be supported using a small amount of memory and bandwidth. A new IETF workgroup was created under the name of ROLL (Routing Over Low power and Lossy networks) to address general routing in LoWPAN networks and the requirements [18][21] caused by the implementation of the new 6LoWPAN adaptation layer in these networks. The IETF-ROLL WG proposes the routing protocol RPL (Routing Protocol for Low power and lossy networks) defined in the RFC 6550 [7], it is based on the distance-vector routing protocol algorithm. The distance-vector protocol considers that each router has a routing table indicating, for each destination network, the local interface to reach it and the best distance associated with it. The choice of using a distance vector algorithm is logical as the use of Link State algorithm is almost impossible in this kind of networks,

Link State cost is very high in terms of computing and memory capacities since each state change, an update message should be distributed to all network nodes. This creates a huge traffic, especially in LoWPAN networks where the propagation conditions change the network status frequently.

3. RPL operation

The RPL protocol is based on the concept of DAG (Direct Acyclic Graph) to avoid creating loops in the tree constructed by distance vector algorithm. RPL has the ability to construct multiple paths back to the same destination and sets alternative routes whenever default routes are inaccessible. This protocol will target resource-constrained networks in terms of energy, power, bandwidth and they have a high probability of packets loss and a very significant error rate.

RPL builds a DAG based on a root node called LBR (Low power and lossy Border Router), usually it is the border router responsible for management of a particular field of nodes and locate in junction of two networks.

LBR, rank 1, is the source of the directed acyclic graph. This LBR and all upper level devices form a DODAG (Destination Object Directed Acyclic Graph), i.e. the construction of a DAG routed to a single destination.

LBR sends an information message DIO (DOADAG Information Object) in multicast. When a device receives a new version of DIO, it calculates its particular rank (compared to the one it just received) and propagates its DIO. From the device point of view, all equipment having a lower rank can be parents. Optimal routes (parents) in the DAG are obtained from metrics and constraints.

LBR periodically transmits DIO messages to update the DAG. When a device joins the network or loses the link to its "parents", it can wait for the next DIO (from a minute to an hour) or request a DIO the solicitation message DIS (DODAG Information solicitation). DIO messages are sent with the Trickle algorithm. This algorithm mainly defines two things: a sequence number that indicates whether the received information is an update, and the delay between each information transmission (which varies depending on settings). These RPL control messages follow the format of the ICMPv6, which has a field in its header that defines the DIO message type (DAG metric container, Destination Prefix, DAG configuration), DAO or DIS.

The concept that each node selects more than one "parent" node by DAG gives flexibility to RPL for self-healing by allowing it to adapt and overcome to topology changes.

We obtain by RPL a topology in two forms: a hierarchical structure by the creation of the parent-child relationship between the nodes, and the mesh topology by the possibility of routing between nodes of the same rank.

RPL can benefit from ND-6LoWPAN protocol [13], the adapted version of the ND protocol (Neighbour Discovery) [14] used by IPv6, responsible for the discovery of other hosts on the same link, determining their address and identifying present routers. The advantage of ND is that it provides useful information such as routing information on one-hop node, maintaining its cache information and maintaining routing information cache itself. This allows the RPL to have a self-configuration when needed.

ND also helps RPL for the diffusion of its DIO messages across the network through the two allowed transmission directions: in the "downward" direction from the root to other nodes in broadcast transmission and in the opposite direction the "upward" from one node to the root in unicast transmission.

4. Denial of Service threats

4.1. DoS definition

Denial of Service (DoS) attacks aim to make a machine or a network unavailable for a certain period. The general principle of DoS attacks is sending data or packets whose size or content is unusual to cause unexpected reactions of the network or targeted node, sometimes they can even cause the service interruption.

This kind of attack is very common on networks because it is simple to implement and can nevertheless have devastating consequences. In addition, the detection and prevention of these attacks are very difficult because they can take many forms.

The basic attacks type are whose targeting the consumption of the bandwidth, the consumption of the processor time or the memory storage ability, creating a congestion in communication links between nodes, the disruption of a component, a service, a routing information or all the system, etc. As like we say in previous section, the 6LoWPAN resource constraints make its routing protocol vulnerable to DoS attacks and easy to disrupt. The paper focus further on in this document on DoS attacks targeting the routing protocol.

4.2. DoS attacks

We give a summary based on an analytical study of [9] , [10] and [22] concerning different DoS attacks that an attacker can use to interrupt the LoWPAN network operation, and more specifically the operation of its routing.

4.2.1. Identity attacks (spoofing)

In the identity attack, also called "Spoofing attack", the attacker aims to damage the data routing within the network that are controlled through the identity of nodes (Fig. 2).

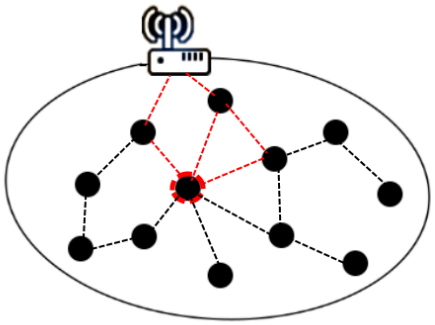

Fig. 2: Spoofing attack

With a valid ID, the attacker can participate in a malicious way in exchange routing data by changing this information or distributing false information.

4.2.2. Sybil

Sybil attack is a kind of identity attacks where the attacker imitate several identities. Like that, it will have more influence on the network and will be able to falsify communications nodes topology from P2MP (Point-to-multipoint) to MP2P (Multipoint-to-point) (Fig. 3).

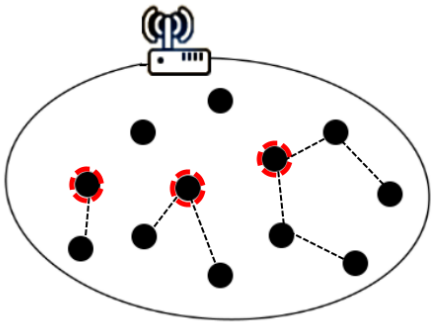

Fig. 3: Sybil attack

4.2.3. Selective forwarding

Selective Forwarding (Selective transmission) attack occurs when the malicious node tries to route all packets transmitted to a node to remove one of these packages, either randomly or according the importance of data contained in this package. The attacker must have a complete idea of the content of the data flowing through the network.

If all these packages are destroyed by malicious node, called the attack: "Black hole" attack (Fig. 4).

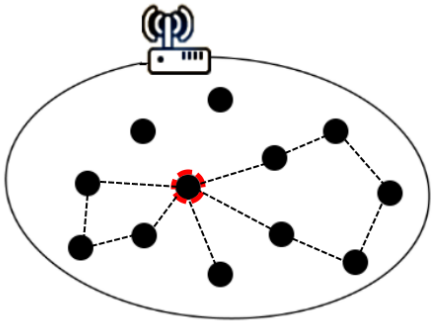

Fig. 4: Black hole attack

4.2.4. Wormhole

The Wormhole attack is produced by at least two malicious nodes that communicate with each other through a different frequency than the network in which they operate so that communication between them still discreet relative to other nodes.

One of these nodes is placed near the Border router and the other a little further, when one receives packets it transmits them directly to the other without passing through the normal path; i.e. through the network nodes. In this way, the malicious nodes can manipulate the packets; they disrupt the network routing since routing protocol data will not reach all the nodes (Fig. 5).

This attack can also be performed using one attacker node, wherein the malicious node distributes packets between two legitimates nodes located far from each other; in order to convince them they are neighboring nodes.

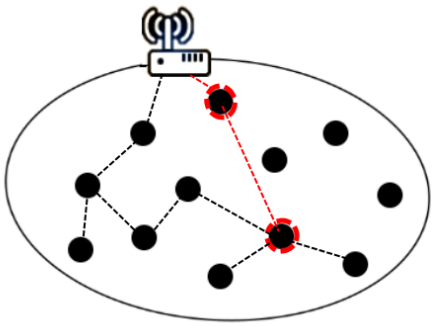

Fig. 5: Wormhole attack

4.2.5. Sinkhole

In a Sinkhole attack, the node tries to attract to it the most possible routes to control over most of the data flowing through the network. The attacker must appear to others as being very attractive by presenting optimal routes (Fig. 6).

4.2.6. Replay routing information

In this attack, the attacker aims to transfer routing information, which aim to determine the topology of the network and update nodes routing tables, in a way that the information be incorrect and thus the disturbance of the network routing.

4.2.7. Hello flood

The origin of the HELLO Flood attack is the routing protocol that requires that neighboring nodes on the same network exchange occasionally HELLO messages to announce their presence and availability. The HELLO message

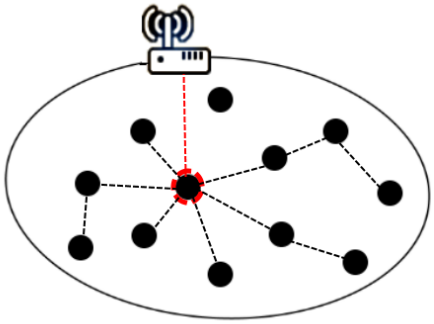

Fig. 6: Sinkhole attack

is used to discover the route and update the routing tables of neighboring nodes. The node that receives this packet, it considers it is in the neighboring (within the scope of the radio emission) of the sender node. An attacker can use a powerful machine and sends a huge number of HELLO packets to different nodes, so that they will consider it as their neighbor node, they will try to transmit their data to this machine, and therefore the loss of these packets (Fig. 7).

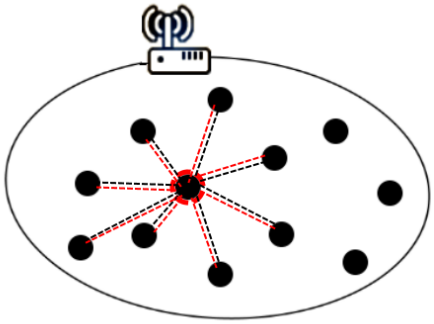

Fig. 7: Hello flood attack

4.2.8. Overload

In this attack, the node overload the network with traffic without any specific content to exhaust the energy of nodes rapidly (Fig. 8).. This can be done by many manners like making routes longer, occupy the nodes and make them unavailable to exchange routing information, etc.

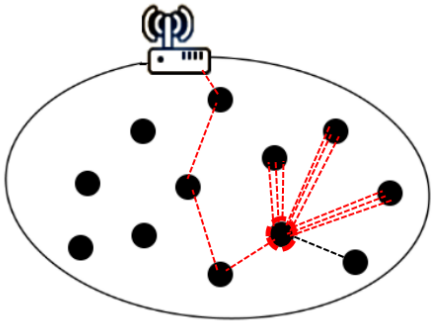

Fig. 8: Overload attack

5. Countermeasures

5.1. General countermeasures

To protect 6LoWPAN network from a DoS attack targeting its routing protocol RPL, a set of measure should be considered [9], the system must have an authentication mechanism of different communication parts, where each node must be authenticated by other nodes to ensure its identity.

To send the same message, the routing protocol must establish several possible routes before to circulate this message. A network node must decide dynamically between several neighboring nodes that will be its next hop to forward its messages. Between a transmitter and receiver, we must not establish only one route between them but several ones to make the network tolerable to routes faults.

Data integrity must be assured, because a single change in the synchronization messages parameters of routing protocol will cause its dysfunction. We should have a mechanism that checks the integrity of these data. We must filter the data that is allowed to be circulated in the network; according to is operation and its environment. In addition, we must ensure the freshness of each message before sending it. These mechanisms will ensure the reliability of exchanged between data the nodes to synchronize their routing parameters.

However, sometimes even with reliable data and authenticated nodes, there are attacks that target the lack of resources and energy for data processing in 6LoWPAN networks, so they aim to flood the network with useless data and put it out of service. Most of DoS attacks use this way, as it does not require strong knowledge. To counter these attacks, there must also be other mechanisms; we must limit the traffic rate among nodes based on the network usage in both cases: by the number of transmitted and received messages, and if it detects nodes that exceed this limit, they must be isolated directly from the network and prohibit them to communicate with other nodes, which is the role of intrusion detection systems (IDS) introduced hereinafter.

5.2. Intrusion detection

Intrusion detection is a security approach that is based on analyzing network data collected in order to detect signs of intrusion or attack to trigger an alarm and discover the anomaly.

There are different kinds of Intrusion Detection Systems (IDS) divided in three types of intrusion detection; misuse IDS, anomaly-based IDS and specification-based IDS. They differ by their mechanism of discovering malicious nodes. Misuse IDS defines firstly patterns of each type of attack that the IDS should detect. If a suspicious behavior match the pattern, it will raise an alarm. Anomaly-based IDS has a start-up phase where it gathers information about the normal behavior of the monitored network. After that, it determines a threshold that if it is exceeded by a suspicious behavior, the IDS raise an alarm. Specification-based IDS is very similar to anomaly-based IDS, the difference is that its threshold is defined a priori.

A number of data features were proposed to be monitored by the IDS in LoWPAN networks [23], they suggest to monitor the time between two consecutive messages, changes on payload, the high delay, repetition, sender identification, collisions, lost packets, modified packets and the amount of energy.

More details about the compatible IDS with 6LoWPAN-RPL characteristics is given in the next section.

6. Intrusion Detection System

To design efficient IDS for 6LoWPAN-RPL, we must respect its characteristic [11]. Firstly, 6LoWPAN networks are heterogeneous infrastructure-less ad hoc networks, mostly distributed in hostile environment difficult to access by a human user, with a high node density. In addition, their resources in terms of processor, memory, storage capacity and bandwidth are very low. Their batteries are more constrained and very sensible to energy exhaustion.

6LoWPAN applications are various; the monitored data is very specific. We cannot obtain an IDS that monitor all attacks parameters because the variation between different application scenarios and the nodes are limited in resources. The IDS must choose indeed, depending the application scenario, the most harmful and dangerous attacks that must be monitored. However, to secure the RPL, the IDS must implement detection mechanisms that deal with DoS threats. The most of DoS attacks aim directly for damaging routing protocol. To choose the adequate IDS, three essential questions must be answered, depending the network type and the concerned application: What type of IDS to use? Where to implement IDS agents? What parameters to monitor? In the next paragraphs, the paper try to answer this question putting the 6LoWPAN network and the RPL protocol as the starting point.

6.1. What type of IDS

As we said in the previous section, there is about three types of IDS; misuse, anomaly-based and specification-based. Misuse IDS defines patterns of the known attacks, so it needs a lot of database analysis to detect an attack, and it is not detecting new attacks as it depends on its pre-deployed database. Anomaly-based depend on its classification of the normal network behavior, which it defines it in its training phase during the start-up period. Specification-based specifies normal network operations that must be defined by a specialist. A suitable IDS for 6LoWPAN that is the one that consumes less resources and flexible in detecting new attacks. Misuse and specification-based consumes less energy as they are based on pre-defined patterns, but they are inflexible in upgrading. Anomaly-based is more suitable because it has the possibility to detect new attacks by developing its threshold in its training phases, and it consumes less energy too. Even though, anomaly-based has the inconvenient that its false-alarm rate is high in detecting a misbehavior of some nodes due, to different external or internal factors, as malicious operation. An IDS that combine between the anomaly-based technics and specification-based technics will decrease the false-alarm rate. Specification-based IDS should use RPL specification as a database for a normal operation. It will be benefic as the DoS attacks target the routing protocol. In the other hand, the IDS will need fewer resources and little communication overhead, as it will use an existing protocol.

6.2. Where to implement the IDS agents

There is three approaches where the IDS agents can be implemented: the network-based approach, the host-based approach and the distributed approach. The distributed approach is more suitable for 6LoWPAN networks. In the network-based approach, the agent is localized at the base station where it analyzes all the traffic sent by the network nodes, which creates a lot of communication overhead. The node-based approach implement agent in every node, which consumes a lot of nodes resources and energy. The distributed approach was founded to deal with network and hot-based approaches, also to benefit from their advantages, as the agent will be implemented in the two levels: in the base station and in all (or some) network nodes. Using the base station is to benefit from its strong resources ability, and using agents in nodes is to reduce monitored traffic and detect locally attacks.

RPL separates the network in levels creating a tree with the parent-child relationships and making the border router in the high level as the base of the tree. Basing on that, and to reduce nodes resources use, instead of that a node monitor all its neighboring nodes, a node monitor only the nodes where it has a direct relationship with them, i.e. its parents or its children. The results of monitored data can be sent to the agent implemented in the base station to compare between them and gives the final decision to revoke or not the suspicious node(s), basing on statistical data and intelligence analysis.

6.3. What parameters to monitor

In the previous section, the paper has discussed some properties that IDS must monitor; it depends on the application and the network environment. To get the properties to be monitored, we must determine the attacks and their symptoms. Through DoS attacks explained in the previous section; targeting routing protocol operations, we can extract the signs and symptoms that the IDS should monitor. Explained threats are sybil, selective forwarding, black hole, wormhole, sinkhole, replay routing information, hello flood and overload attacks.

Commonly used measures are token to detect misbehavior characteristics resulting from these attacks. These measures are received signal strength, packet sending rate, packet receiving rate, packet delivery ratio, packet acking, packet send ratio, packet dropping rate, packet forwarding rate and carrier sensing time.

- Received signal strength is the measure of the power contained in a received radio signal.
- Packet sending rate is the packets number sent in a predefined period.
- Packet receiving rate is the packets number received during a predetermined period.
- Packet delivery ratio is the ratio of packets that are successfully delivered based on the packets number that were sent by the sender.
- Packet acking rate is the acknowledgments number that been sent to a node.
- Packet send ratio is the ratio of packets that are successfully sent to the packets number that must be sent.
- Packet dropping rate is the packets number sent to a node but were been forwarded by it.

- Packet forwarding rate is the packets number received by a node from another; to forward them to another node during a predefined period.

- Carrier sensing time is the amount of the waiting time spent by a node to access to the channel.

These parameters and others should be monitored by nodes agents, collected data could be sent to the base station to take a decision based on statistics from old received data.

7. Conclusion

This paper presented a review of denial of service issues in 6LoWPAN network, making the focus on attacks targeting its underlying routing protocol RPL and the IDS solution as the most suitable countering this type of attacks. First, the paper gives an overview of 6LoWPAN network, its architecture and its operation protocols. Also the paper presents the RPL protocol, that was proposed to solve routing issues created by 6LoWPAN features that have many constraints such as energy consumption, long nodes sleep cycles, the quality of service, the necessity of supporting different types of addressing (unicast, multicast, anycast), supporting mobility, etc, using a small amount of memory and bandwidth. The paper presents in detail RPL operation, especially how its construct its routes schema by constructing a DoDAG (Destination Object Directed Acyclic Graph); a schema that arrange the network nodes in ranks binding them by a parent-chlid relationship. The paper discusses RPL security issues resulting from 6LoWPAN low resources; making the focus o denial of service attacks (DoS) as they are the most harmful attacks. The paper chose to deal with DoS attacks targeting the routing protocol, the threats presented in this document are identity, sybil, selective forwarding, black hole, wormhole, sinkhole, hello flood and overload attacks.

Then, the paper reviews the main countermeasures must be token to protect 6LoWPAN-RPL from DoS threat. Solutions are presented in two parts, the first part gives general mechanisms and recommendations as the necessity of assuring data integrity and nodes authenticity, establishing several routes between two nodes, filtering the data that is allowed to be circulated in the network, limiting the traffic into the network and the entering one from the internet side, etc. As all of these measures will not be effective in the case of a malicious node, the second part treats the intrusion detection concept and its different systems.

Finally, the paper discusses the issues of applying IDS in 6LoWPAN networks trying to answer the main questions of designing an intrusion detection. The first question is about the type of IDS to chose to design between the misuse, anomaly-based and specification-based IDS. The second concerns the placement of the IDS agents between network-based approach, nodes-based approach and distributed-based approach. The final and third question is about the parameters that the IDS should to monitor to deal with DoS attacks, the paper resumes these parameters in received signal strength, packet sending rate, packet receiving rate, packet delivery ratio, packet acking rate, packet send ratio, packet dropping rate, packet forwarding rate and carrier sensing time.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, Future Gener. Comput. Syst., vol. 29, no. 7, pp. 16451660, Sep. 2013.

[2] G. Yang and F. Li, Investigation of Security and Defense System for Home Based on Internet of Things, in 2010 International Conference on Web Information Systems and Mining (WISM), 2010, vol. 2, pp. 812.

[3] G. Shen and B. Liu, The visions, technologies, applications and security issues of Internet of Things, in 2011 International Conference on E -Business and E -Government (ICEE), 2011, pp. 14.

[4] C. P. P. Schumacher, N. Kushalnagar, and G. Montenegro, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals. [Online]. Available: https://tools.ietf.org/html/rfc4919.

[5] N. Kushalnagar, G. Montenegro, D. E. Culler, and J. W. Hui, Transmission of IPv6 Packets over IEEE 802.15.4 Networks. [Online]. Available: http://tools.ietf.org/html/rfc4944.

[6] J. A. Gutierrez, M. Naeve, E. Callaway, M. Bourgeois, V. Mitter, and B. Heile, IEEE 802.15.4: a developing standard for low-power low-cost wireless personal area networks, IEEE Netw., vol. 15, no. 5, pp. 1219, Sep. 2001.

[7] T. W. ¡wintert@acm.org¿, RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. [Online]. Available: http://tools.ietf.org/html/rfc6550.

[8] A. Rghioui, M. Bouhorma, and A. Benslimane, Analytical study of security aspects in 6LoWPAN networks, in 2013 5th International Conference on Information and Communication Technology for the Muslim World (ICT4M), 2013, pp. 15.

[9] R. K. Alexander, M. Richardson, T. Tsao, V. Daza, A. Lozano, and M. Dohler, A Security Threat Analysis for Routing Protocol for Low-power and lossy networks (RPL). [Online]. Available: http://tools.ietf.org/html/draft-ietf-roll-security-threats-07.

[10] A. Wood and J. . Stankovic, Denial of service in sensor networks, Computer, vol. 35, no. 10, pp. 5462, Oct. 2002.

[11] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach, Int. J. Commun. Syst., vol. 25, no. 9, pp. 11891212, Sep. 2012.

[12] D. Kyriazis, T. Varvarigou, A. Rossi, D. White, and J. Cooper, Sustainable smart city IoT applications: Heat and electricity management amp; Eco-conscious cruise control for public transportation, in World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a, 2013, pp. 15.

[13] S. Chakrabarti, Z. Shelby, and E. Nordmark, Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). [Online]. Available: http://tools.ietf.org/html/rfc6775.

[14] T. Narten, W. A. Simpson, E. Nordmark, and H. Soliman, Neighbor Discovery for IP version 6 (IPv6). [Online]. Available: https://tools.ietf.org/html/rfc4861.

[15] M. Felsche, A. Huhn, and H. Schwetlick, Routing Protocols for 6LoWPAN, in IT Revolutions, M. L. Reyes, J. M. F. Arias, J. J. G. de la Rosa, J. Langer, F. J. B. Outeirio, and A. Moreno-Munoz, Eds. Springer Berlin Heidelberg, 2012, pp. 7183.

[16] G. K. Ee, C. K. Ng, N. K. Noordin, and B. M. Ali, A Review of 6LoWPAN Routing Protocols, Proc. Asia-Pac. Adv. Netw., vol. 30, no. 0, pp. 7181, Dec. 2010.

[17] V. Kumar and S. Tiwari, Routing in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN): A Survey, J. Comput. Netw. Commun., vol. 2012, p. e316839, Mar. 2012.

[18] J. Martocci, P. Mil, N. Riou, and W. Vermeylen, Building Automation Routing Requirements in Low-Power and Lossy Networks. [Online]. Available: http://tools.ietf.org/html/rfc5867.

[19] A. Brandt and J. Buron, Home Automation Routing Requirements in Low-Power and Lossy Networks. [Online]. Available: http://tools.ietf.org/html/rfc5826.

[20] S. Dwars, T. Phinney, and P. Thubert, Industrial Routing Requirements in Low-Power and Lossy Networks. [Online]. Available: http://tools.ietf.org/html/rfc5673.

[21] M. Dohler, D. Barthel, T. Watteyne, and T. Winter, Routing Requirements for Urban Low-Power and Lossy Networks. [Online]. Available: http://tools.ietf.org/html/rfc5548.

[22] M. J. Handley and E. Rescorla, Internet Denial-of-Service Considerations. [Online]. Available: http://tools.ietf.org/html/rfc4732.

[23] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. Ruiz, and H. C. Wong, Decentralized Intrusion Detection in Wireless Sensor Networks, in Proceedings of the 1st ACM International Workshop on Quality of Service Amp; Security in Wireless and Mobile Networks, New York, NY, USA, 2005, pp. 1623.