Hindawi Publishing Corporation
Journal of Sensors
Volume 2016, Article ID 5017248, 13 pages
http://dx.doi.org/10.1155/2016/5017248

Research Article

Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks

Katarzyna Mazur,[1] Bogdan Ksiezopolski,[1] and Radoslaw Nielek[2]

[1]*Institute of Computer Science, Maria Curie-Sklodowska University, Pl. M. Curie-Sklodowskiej 5, 20-031 Lublin, Poland*
[2]*Polish-Japanese Academy of Information Technology, Koszykowa 86, 02-008 Warsaw, Poland*

Correspondence should be addressed to Katarzyna Mazur; katarzyna.mazur@umcs.pl

Received 24 March 2016; Accepted 29 May 2016

Academic Editor: Fei Yu

The growing popularity of wireless sensor networks increases the risk of security attacks. One of the most common and dangerous types of attack that takes place these days in any electronic society is a distributed denial of service attack. Due to the resource constraint nature of mobile sensors, DDoS attacks have become a major threat to its stability. In this paper, we established a model of a structural health monitoring network, being disturbed by one of the most common types of DDoS attacks, the flooding attack. Through a set of simulations, we explore the scope of flood-based DDoS attack problem, assessing the performance and the lifetime of the network under the attack condition. To conduct our research, we utilized the Quality of Protection Modeling Language. With the proposed approach, it was possible to examine numerous network configurations, parameters, attack options, and scenarios. The results of the carefully performed multilevel analysis allowed us to identify a new kind of DDoS attack, the delayed distributed denial of service, by the authors, referred to as DDDoS attack. Multilevel approach to DDoS attack analysis confirmed that, examining endangered environments, it is significant to take into account many characteristics at once, just to not overlook any important aspect.

1. Introduction

Wireless sensor networks (WSNs) are becoming an increasingly growing topic of conversation both in the scientific world and outside of it. As WSN continues to expand, it opens the door to a lot of opportunities, but also to many challenges. Security concerns are the issues being often times brought up: besides the security threats, we have the issue of privacy and data sharing. Unfortunately, the rapid growth of WSN is not always accompanied by a rapid improvement of efficient security solutions, giving criminals new opportunities to explore this technology as new attack vectors. One of the most common and dangerous types of attack that takes place these days is a distributed denial of service (DDoS). Distributed denial of service attacks are defined as attacks launched from multiple ends of a wireless sensor network, towards a set of legitimate nodes, with the intent of exhausting their limited resources. DDoS attacks can take on many forms, depending upon the target system and objectives of the attacker, but they all have the same goal: these attacks significantly affect the performance of the network and eventually lead to complete paralysis of network operation. As network devices proliferate, vulnerabilities could enable attackers to assemble a large number of nodes to use in such attacks. If the attack is powerful enough, sensors will fail in serving their functions normally, becoming unreachable, so even legitimate users cannot use them. While this intense strain is taking over devices, hacker can try to slip into the back door unnoticed. That is the reason why security needs to be backed into wireless sensor networks from the initial design phase; it needs to be built in as the foundation of WSN environments, with rigorous validity checks, authentication, and data verification, and all communication needs to be encrypted. In light of the importance of what sensors have access to, it is essential to understand their security risks.

However, practical experiments with distributed denial of service attacks are difficult, because the scope of attack sources spreads in a wide geographical area and experiments in the local network can be insufficient to illustrate the real situation. Moreover, DDoS attacks require plenty of

controlled devices and therefore make difficulties in getting a sufficient amount of infected and ready to attack machines under the laboratory conditions. Instead of performing the real execution of distributed DoS attacks, their examination can be done using different modeling methods and tools. Modeling allows making the estimation of the influence of different attack properties with less time and resource supplies. It provides a test-bed to evaluate the costs and consequences imposed by various attack scenarios and defenses.

As WSN is especially vulnerable against external and internal attacks due to its peculiar characteristics, it should comply with certain security requirements, such as confidentiality, integrity, and authentication, derived from the application context. However, deploying security in WSN is a complex and time-consuming process, which seeks to accommodate frequently competing factors, such as functionality, scalability, or simplicity. In such case, the multilevel analysis is essential: it provides a better understanding of the security threats problem and allows for examining it from miscellaneous points of view.

In this paper, we contribute to solving the problem of the analysis of wireless sensor network environments, which struggle with flood-based distributed denial of service attack. The main contributions of this paper are summarized as follows:

(1) We performed a multilevel analysis, in which we examined the influence of the number of compromised sensors on sink's performance. To conduct our research, we prepared and implemented distributed denial of service model in Quality of Protection Modeling Language (QoP-ML) [1], to be able to analyze how different properties of the attack influence its success probability.

(2) An approach proposed in this paper was utilized in a case study of structural health monitoring of historical buildings, which represents critical systems, which need constant and careful monitoring. Through a set of performed simulations, we determined the energy consumption of wireless sensors deployed in critical points of the building structure, disturbed by a DDoS attack. Further, we estimated the lifetime of a base station, identifying another aspect of the multilevel analysis: the influence of DDoS attack on energy resource exhaustion, defining a new kind of DDoS attack, *DDDoS*, defined by the authors as the *delayed distributed denial of service* attack.

(3) Another contribution of this paper is the QoP-ML model of WSN under the DDoS attack, prepared for our case study. This model can be used for testing how well existing mitigation methodologies perform and how they can be improved to prevent DDoS occurence. With the proposed approach, we can systematically investigate and characterize how to provide denial of service defenses at the lowest (performance, energy, and finance) cost, satisfying the availability of network connections during the attack and assuring defined security objectives at the same time.

The multilevel analysis utilized in this paper is an innovative and unique evaluation method, which allows for taking into account not only sink's performance, but also the energy consumption. Using Quality of Protection Modeling Language, we are able to build a single model and consider it in many terms, such as the quality of protection, effect on the environment, or the influence on financial and economic performance. In this paper, we focus on time and energy consumption analyses.

The remainder of this paper is divided into six sections. In Section 2, we include the related work about distributed denial of service modeling. We try to compare our approach to those available in the literature, briefly discussing Quality of Protection Modeling Language. Moving on to Section 3, we examine an example network architecture and its components and dynamics, together with describing the most essential elements of analyzed environment. Turning on to Sections 4 and 5, we focus on modeling, simulation, and analysis of gathered results and conclude with Section 6, in which we summarize our work.

2. Related Work

The problem of distributed denial of service attacks is not new to the literature. However, every published view of this type of attack is somewhat different. Some authors examine the denial of service attacks from the OSI or TCP/IP reference models point of view [2–4] providing a comprehensive taxonomy of DDoS attacks [5–7]. Others try to use miscellaneous modeling tools to analyze distributed denial of service [8–11], while some focus on detection and mitigation techniques [12–15].

Although the literature on DDoS is more than rich, only a few authors consider formal modeling of DDoS attacks in wireless sensor networks [15–19]. To compare and organize all the existing approaches to denial of service formal modeling, we prepared a set of requirements which, if met, allow for an in-depth and detailed analysis of proposed methods in terms of their usefulness and efficiency. The modeling approach, to be considered a valuable, functional, and effective framework, should possess defined set of qualities. In Table 1 we investigated different approaches available in the literature and assessed them taking into account selected attributes. A proposed set of modeling qualities along with their explanations are presented below:

(i) *Analytical Representation (AR)* refers to the mathematical representation of the model, defines if the model is represented in mathematical and analytical ideas (providing logical relationships and formulas), and moreover specifies the capability of being executed and support of automated tools being able to execute the model.

(ii) *Universality (U)* determines if the given approach is a general purpose approach (can be utilized for building and analyzing models not only of wireless sensor networks).

(iii) *Performance Evaluation (PE)* gives the possibility of performance evaluation of the analyzed system.

Table 1: Comparison of existing DDoS modeling approaches.

Approach	Characteristic							
	AR	S	PE	F	MA	C	SCL	EE
Dines Kumar and Navaneethan [15]	√	—	√	√	—	√	√	√
Chen et al. [16]	√	√	√	—	—	√	√	—
Eian and Mjølsnes [17]	√	√	√	—	—	√	√	—
Dini and Tiloca [18]	√	—	√	√	—	√	√	—
Zhang et al. [19]	√	—	√	—	—	√	—	√
QoP-ML's approach	√	√	√	√	√	√	√	√

(iv) *Flexibility (F)* concerns the ease of adaptation to introduced changes; modeling approach is considered *flexible* if changes in real environment can be easily applied to existing models.

(v) *Multilevel Analysis (MA)* allows taking into account lots of different attributes, components, and aspects of the considered system during the modeling process.

(vi) *Consistency (C)* stands for the ability to model the system maintaining its states and communication steps consistency.

(vii) *Scalability (SCL)* is the capability of an approach to handle a growing amount of model components, or its potential to be enlarged in order to accommodate that growth. The approach is *scalable* if it allows analyzing architectures of any size.

(viii) *Energy Evaluation (EE)* allows for evaluation of the of energy efficiency of the analyzed system.

In [15] authors proposed an algorithm for *incorporated cryptographic mechanism and clustering method for preventing DoS attacks*. Due to the fact that the mechanism is described in a form of organized steps, it satisfies the *Analytical Representation* criteria. In the paper, researchers do not mention if it is possible to use proposed mechanism in different environments (hence, it does not pose the *Universality* requirement). In their work, scientists present performance results (*Performance Evaluation*), mentioning the *Energy Evaluation* as well. Their approach is *flexible*, *scalable*, and *consistent*, but it is not entirely *Multidimentional* (for instance, it does not take into account economic or ecological point of view and considers only a limited set of network characteristics).

Building a DDoS attack cost model based on mathematical equations, authors in [16] answered questions about *Analytical Representation* and *Consistency*. Presenting simulation results, they discuss *Performance Evaluation*; however, they do not say a word about *Energy Evaluation*. Proposed approach can act as a general purpose approach (can be implemented in any type of network), since it relies on numerical results (*Universality*). However, due to the fact that the model requires much computation, it is quite *inflexible*. When it comes to *Multilevel Analysis*, research introduced in [16] considers only defined group of examined variables. Numerical representation of the model makes it *scalable*.

When it comes to formal DDoS modeling methods, in [17] scientists proposed a formal method for modeling semantic DoS attacks against wireless networks and showed how the model can be used to discover protocol vulnerabilities. Their approach relies on formal description and analysis (*Analytical Representation*). The method is *scalable*; however, it is quite *inflexible* (due to its formalism and accuracy). The authors consider *Performance Evaluation* and introduce the cost model but do not mention *Energy Evaluation*. Same as in the case of previously discussed works, *Multilevel Analysis* is also not satisfied.

Since an approach introduced in [18] provides an attack specification language, compiler, and simulator, it automatically satisfies the *Analytical Representation* criteria. (Because the model is defined as a set of logical rules (algorithms), it can be considered as *Analytically Represented*.) However, the solution presented in [18] does not pose the *Universality* characteristic, because it is designed only for wireless sensor networks. It is noteworthy that using *ASF* it is quite straightforward to make changes in the existing model (*Flexibility*), as well as handling its growth (*Scalability*). Regarding *Multilevel Analysis*, [18] does better than remaining approaches; however, it does not cover all the demands that a real deployment environment would require.

Another approach which makes use of algorithms is presented in [19] (*Analytical Representation*). Here, the authors proposed a novel Message Observation Mechanism (MoM) for preventing DoS attacks. This mechanism utilizes a similarity function which is based on spatiotemporal correlation for identifying the frequency attacks and content attacks. Nevertheless, in the article, researchers do not give all mechanisms of reroute and rekeys, making the approach *unscalable* and *inflexible*. Although the authors mention *Energy Evaluation* (and *Performance Evaluation*), they do not refer to other analysis dimensions (*Multilevel Analysis*). Because proposed mechanism is designed for wireless sensor networks, it does not meet the *Universality* requirement.

Although different approaches to distributed denial of service attack exist, there still is a lack of composite denial of service attack model that combines various types of resource exhaustion for a more realistic representation of an attack. Systematic, standardized, and organized methodologies should be appointed to detect, defend, and mitigate against denial of service attacks. A multidimensional, profound analysis, which allows examining miscellaneous aspects of an attack using logical formulas, is the most reliable approach to deal with DDoS. To the best of the author's knowledge, Quality of Protection Modeling Language (QoP-ML), introduced in [20], is the only existing modeling

language which satisfies all these requirements simultaneously. It allows for balancing security against the system efficiency, performing multicriteria analysis and extending the possibility of describing the state of the environment in detail (*Analytical Representation*). Quality of Protection Modeling Language permits determining the required quality of protection (QoP) and adjust some of the security measures to these requirements, together with ensuring efficient system performance (*Performance Evaluation*). This type of profound analysis can be accomplished by the help of the Automated Quality of Protection Analysis tool [1] (*Flexibility*, *Scalability*), which allows for the evaluation of the impact of every single operation defined in the prepared security model in terms of the overall system security. Additionally, in previous works, there were proposed and examined approaches which were successful also in assessing time, energy (*Energy Evaluation*), quality of protection, financial expenditures, and impact on the environment of the analyzed IT environments at the same time. Building a network model in Quality of Protection Modeling Language, one is able to take into account type of the device (thanks to the possibility of using real hardware performance metrics, one can actually use any type of device), communication medium type and its characteristics, network topology, packet flow (routing) (*Multilevel Analysis*) and examine how all these components combined together in different configurations can influence DDoS success probability.

For additional information about QoP-ML itself, its syntax, semantics, algorithms, and capabilities, please refer to [20, 21].

3. Flood-Based Denial of Service Attack Analysis

In this section, we describe a conventional DDoS attack tactic, in which an attacker floods targeted resource with packets. We propose an example network architecture along with scenarios, where we launch a DDoS attack, a type of malicious activity aimed at disrupting the availability of a sink so it can no longer deliver its functionality.

Further, we present and discuss prepared environment in detail, providing more concise representation of utilized devices, routing, medium, network architecture, and topology.

Distributed denial of service flooding attacks are one of the biggest concerns for security professional. They are typically explicit attempts to disrupt legitimate motes' access to a sink node. The attackers usually gain access to a large number of sensor devices, by exploiting their vulnerabilities to set up attack armies. Once an attacking army has been set up, an attacker can invoke a coordinated, large-scale attack against one or more gateways. A flooding-based distributed denial of service attack sends a large amount of unwanted traffic to a victim sink. This results in consuming large amounts of its resources in order to maintain a very large list of connections, eventually leading to the device running out of resources and becoming unable to provide normal services. In the case of flood-based DDoS attack, the attacker must be in control of a large number of nodes which can be instructed to execute specific requests to the target sink, in a synchronized manner and for a specific period of time. The so-called "bots" are compromised sensors, used by the attacker. Once a trigger is sent from the attacking node, the bots will execute the designated requests and the attacker will rely on the sheer number of requests/second to bring the sink's processing power to its knees, causing it to cease responding to legitimate sensors. The existence of a vulnerability is not a precondition of this type of attack, in the sense that the attack does not rely on vulnerabilities to execute. However, controlling a large "army" of bots usually implies exploiting vulnerabilities.

For a more concise representation of our approach to DDoS attack analysis, we proposed expressing it through a set of key points, on which we elaborate in the following sections.

3.1. Utilized Protocols. The network deployed in [22] is an exmaple of an insecure network, as it does not ensure any security attributes; packets traversing the network are unencrypted. In our case study, we intend to evaluate the influence of security attributes on the performance of the network, from the time and energy point of view. We introduced two protocols, which guarantee two different levels of security: *no security* (with no encryption) and *security* (where we use AES to encrypt the data).

In the *no security* level protocol, sensors start measurement and send the acceleration data (the result of the measurement) to the sink node for further processing. In this protocol level, no security attributes are guaranteed.

The *security* level protocol introduces confidentiality of accelerated data. After measurement, sensors encrypt the data with a predeployed network key. In this protocol, the AES algorithm is chosen for the encryption in the CTR (CTR stands for *counter* and represents a mode of operation, which uses a block cipher to encrypt messages of arbitrary length in a way that provides confidentiality or authenticity) mode and with the key size equal to 128 bytes.

3.2. Network Architecture and Topology. For example, hypothetical deployment of wireless sensors inside a heritage building, which we examine in this paper, is pictured in Figure 1. Our example network is based on the one presented in [22]. Here, wireless sensors, located in critical points of the building structure, measure required physical quantities (such as vibrations, temperature, or humidity). Data collected by nodes flow into the base station where further data compression and analysis are performed. In such a network architecture, the sink node is a bottleneck and a single point of failure. Proper operation of the base station is crucial for the entire network. Once the sink node fails, the whole network will be paralyzed. In our simulation scenarios, we distinguished 3 types of sensor nodes: compromised sensors, sink node (also known as the gateway or base station), and attacker node. Because the function of legitimate sensors is to take the measurements and send the data to the base station several times during an hour, their operation does not influence much DDoS attacks which last for a few minutes. Due to the fact that the traffic they generate is quite

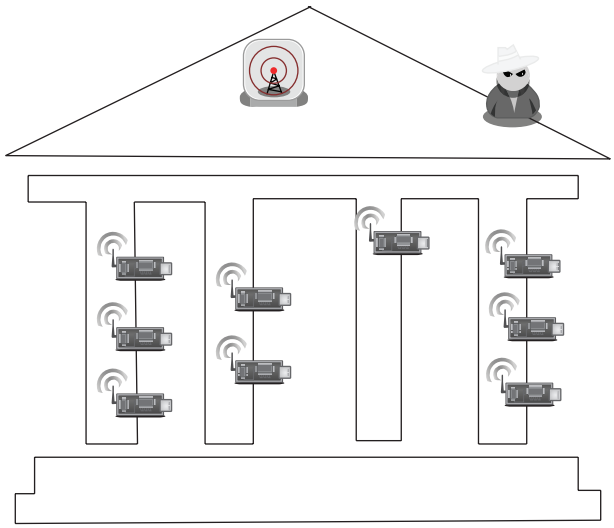

Figure 1: Example network considered for a distributed denial of service attack model.

imperceptible from DDoS attack point of view, we decided to focus only on compromised nodes, the sink node, and the attacker node preparing our model. In order to obtain realistic results, we assumed that all the utilized sensors (compromised sensors, sink node, and the attacker) are TelosB devices, equipped in two AA batteries with 1200 mAh capacity [23]. Because of the flexibility of the QoP-ML, we managed to use the real hardware performance metrics and physical attributes of TelosB nodes and even model its power consumption characteristics.

3.3. Data Flows and Routing. While the primary purpose of a sensor node is data sensing and gathering toward a base station through wireless communication, each of them also has limited processing capabilities that may be exploited, as in the case of an attack. During a normal network operation, sensors continuously monitor the environment, gather relevant data, and send it to the gateway. Data collected from all sensor nodes is uploaded to a sink node and further processed. Considering the attack scenario, network traffic and packet flows increase: attacker takes control of the available sensors (legitimate sensors then become compromised ones) and uses them to generate flooding traffic in order to exhaust sink resources and consequently disturb the whole network. The aggressor knows that if the sink node fails, the entire network will be paralyzed. In our model, we assumed that the attacker communicates with compromised sensors and after every 10 seconds broadcasts a flood message to the devices which he controls. Motes controlled by the attacker in an infinite loop listen for incoming requests (the flood orders) and flood sink with useless messages. Although there is only one packet in each flood wave, attack's power is hidden in the number of compromised sensor devices. It is considered that structural health monitoring network consists of 200 devices. In our simulations, the attacker takes control of 150 (scenarios 1 and 2), 100 (scenarios 3 and 4), 75 (scenarios 5 and 6), and 50 (scenarios 7 and 8) sensors. During the first flood wave, each sensor sends a single packet to the base station (which results in 150, 100, 75, and 50 packets in total). When when the attack escalates, the number of send packets increases, respectively, (resulting in $flood\ wave\ number \times number\ of\ compromised\ sensors$ packets). The more devices attacker has under his control, the more powerful attack is generated.

As for routing information, considered network is a single-hop wireless network in which each station can transmit or communicate directly with the sink node.

3.4. OSI Layers and Protocols. Network and transport layer DDoS attacks can be carried out on a wired or wireless network. The majority of DDoS attacks target the network and transport layers. Such attacks occur when the amount of data packets and other traffic overloads a network or server and consumes all of its available resources. For this reason, during analysis, we focus on layer 3 and layer 4 DDoS attacks, because they are types of volumetric DDoS attacks on a network infrastructure. Layer 3 DDoS (network layer) and layer 4 DDoS (transport layer) attacks rely on extremely high volumes (floods) of data to slow down sink performance, consume bandwidth, and eventually degrade access for legitimate sensors. Our DDoS attack analysis does not refer to a specific protocol but can be applied to all protocols running on the network and transport OSI layers.

3.5. Communication. As mentioned before, the network presented in Figure 1 is a wireless network. Here, all the existing sensor devices use same communication channels to communicate, and the message broadcasted by one of the nodes on the common channel is simultaneously heard by all other motes. In our environment, we consider two air channels: one of them is used by the attacker and compromised nodes, while the other one is responsible for the communication of compromised nodes and a sink node. As the sink node must have some mechanisms to store and forward arriving requests, we assumed that it is equipped with a communication buffer, which is capable of storing a defined number of packets. Sink uses available communication channels to continuously wait for incoming data packets. These packets can be send as a plain text or can be encrypted. When the buffer on the specific channel is full, and there are still requests to handle, they are simply dropped. Under certain conditions, overflow of sink's buffer indicates that the denial of service occurred.

4. DDoS Attack Model in Quality of Protection Modeling Language

Examining a DDoS attack in Quality of Protection Modeling Language, we prepared the model of wireless sensor network discussed above, gathered and utilized real hardware security metrics, and developed different versions of the proposed scenario (Table 2). Modeling DDoS attack, we defined QoP-ML's `functions`, `equations`, `channels`, `processes`, `subprocesses`, and `hosts`. Prepared scenarios (and thus the QoP-ML's security model designed and used in our case

Table 2: Scenarios prepared for DDoS detection and analysis. Considered WSN consists of 200 nodes in total.

Scenario number	Sink type	Buffer size	Number of compromised sensors	Communication type
1	TelosB	192	150	Encryption: AES-CTR 128-bit key
2	TelosB	192	150	No encryption
3	TelosB	192	100	Encryption: AES-CTR 128-bit key
4	TelosB	192	100	No encryption
5	TelosB	192	75	Encryption: AES-CTR 128-bit key
6	TelosB	192	75	No encryption
7	TelosB	192	50	Encryption: AES-CTR 128-bit key
8	TelosB	192	50	No encryption

study) can be downloaded from QoP-MLs project web page [1].

After a brief introduction of the network components and existing traffic flows presented in the previous section, let us now move on to the utilization of our modeling framework, where we discuss abstracted environment in more detail.

4.1. Network Architecture and Topology. Modeling considered network architecture in QoP-ML, we distinguished 3 types of `host` structures, namely, `sink`, `attacker`, and `compromised sensor`. Using one of the QoP-ML's features, known as security metrics, we were able to determine how hardware specifications influence system performance in the case of DDoS attack. We assumed that all sensor nodes (sink, attacker, and compromised sensors) have exact hardware characteristics, taken from TelosB datasheet [23] and previous experiments [24]. Using the `communication` module introduced in [25], we were able to translate existing network topology to QoP-ML as well.

When legitimate sensor becomes an intruder (Listing 1), its main role is to continuously wait for flood orders from the attacker (line (9)). When compromised sensors receive a flood command from an attacker (line (13)), they prepare data (lines (15)-(16)) and depending on the command type included in the message (lines (26)–(34)) generate useless messages (lines (23)-(24)) to flood sink (lines (27) and (33)). Special command type send by the attacker indicates that sensors should stop communicating with sink (lines (36)-(37)). Compromised sensors are also able to encrypt data before transmission (lines (18)–(21)). Such a solution allows determining how this cryptographic process influences attack success probability and assesses how well utilized security mechanisms perform.

Attacking node, modeled in QoP-ML, is presented in Listing 2. It is a special type of device, which, by means of the `mgmt` channel, communicates with compromised nodes. The role of the attacker is to generate a flood command (lines (9)–(21)) and send it through the `mgmt` channel to the compromised mote (lines (11) and (20)). After receiving a flood order from the attacker, compromised sensors start to flood the network with useless traffic. When the attack is

```
(1)  host CompromisedSensor(rr)(*)
(2)  {
(3)
(4)   #MY_ID = id();
(5)   #Attacker_ID = id(Attacker);
(6)   #SINK_ID = id(Sink);
(7)   #KEY = nonce();
(8)
(9)   process MainProcess(*)
(10)  {
(11)   while(true)
(12)   {
(13)   in(ch_MGMT: MESSAGE: |*,*|);
(14)
(15)   DATA = collected_data()[UPDATED];
(16)   save_collected_data(DATA)[UPDATED];
(17)
(18)   subprocess EncCollectedData(*) {
(19)    DATA = (DATA, nonce());
(20)    DATA = s_enc(DATA, KEY)[AES-CTR,128];
(21)   }
(22)
(23)   DATA_MSG = (MY_ID, SINK_ID, data_msg(),
(24)    non_legit(), DATA);
(25)
(26)   if(MESSAGE[2] == msg_flood1()){
(27)     out(ch_WSN: DATA_MSG);
(28)   }
(29)
(30)   %...
(31)
(32)   if(MESSAGE[2] == msg_flood6()){
(33)     out(ch_WSN: DATA_MSG);
(34)   }
(35)
(36)   if(MESSAGE[2] == msg_stop()){
(37)     break;
(38)   }
(39)  }
(40) }
(41) }
```

Listing 1: Compromised sensor node modeled in QoP-ML.

```
(1) host Attacker(rr)(⋆)
(2) {
(3)  #MY_ID = id();
(4)  #SENSOR_ID = id(CompromisedSensor);
(5)  #KEY = nonce();
(6)
(7)  process MainProcess(⋆)
(8)  {
(9)   subprocess FirstFloodWave(⋆){
(10)    FLOOD_MSG = (MY_ID, SENSOR_ID, msg_flood1());
(11)    out(ch_MGMT: FLOOD_MSG);
(12)    wait()[UPDATED];
(13) }
(14)
(15) %...
(16)
(17) subprocess SixthFloodWave(⋆){
(18)  FLOOD_MSG = (MY_ID, SENSOR_ID, msg_flood6());
(19)  out(ch_MGMT: FLOOD_MSG);
(20)  wait()[UPDATED];
(21) }
(22)
(23) STOP_MSG = (MY_ID, SENSOR_ID, msg_stop());
(24) out(ch_MGMT: STOP_MSG);
(25) }
(26) }
```

Listing 2: Attacker node modeled in QoP-ML.

over, attacker informs compromised nodes that they can stop sending messages (lines (23)-(24)).

Sensor, which is subject to a DDoS attack, is modeled in Listing 3. Its function is to handle incoming requests (line (10)), preserve (lines (12)-(13)), and finally process them (line (20)). When the data coming to sink both from compromised motes is encrypted, before processing, sink decrypts data packets (lines (15)–(18)).

Further information about the definition of `hosts`, `processes`, and `subprocesses` structures can be found in [20].

Security metrics utilized in our scenarios concern communication (electric currents in one of the possible node states: listening, sending, and receiving), cryptographic primitives (symmetric and asymmetric encryption), and CPU type. With QoP-ML's metrics it is possible to take into account different hardware characteristics during the simulation process. Such a feature lets one to examine how they influence network performance under an attack. Metrics used by our model are presented in Listing 4. Here we specify the encryption/decryption algorithm, its key characteristics (lines (6)–(10)), and the current of the utilized CPU (lines (12)-(13)). Additional details on security metrics can be found in [20].

Besides defining hardware characteristics, QoP-ML allows for expressing topology of the considered network

```
(1) host Sink(rr)(⋆)
(2) {
(3)  #MY_ID = id();
(4)  #KEY = nonce();
(5)
(6)  process MainProcess(⋆)
(7)  {
(8)  while(true)
(9)  {
(10)  in(ch_WSN: DATA_MSG: |⋆, ⋆, data_msg()|);
(11)
(12)  DATA = DATA_MSG[4];
(13)  save_collected_data(DATA)[UPDATED];
(14)
(15)  subprocess DecCollectedData(⋆) {
(16)    DATA = s_dec(DATA, KEY)[AES-CTR,128];
(17)    DATA = DATA[0];
(18)  }
(19)
(20)  process_data(DATA)[UPDATED];
(21)
(22)  }
(23)  }
(24) }
```

Listing 3: Sink node modeled in QoP-ML.

```
(1) metrics {
(2) conf (TelosB) {
(3)         CPU = 16-bit 8MHz TI MSP430;
(4) }
(5) data(TelosB) {
(6)  primhead[function][alg][key_size][time:block(ms,B)]
(7)         [size:ratio];
(8)  primitive[s_enc][AES-CTR][128][1:34:16][1:1];
(9)  #
(10) primhead[function][alg][key_size][time:block(ms,B)]
(11)         [size:nested];
(12) primitive[s_dec][AES-CTR][128][1:34:16][1:1];
(13) #
(14) primhead[function][current:exact(mA)];
(15) primitive[cpu][2.4];
(16) % ...
(17) }
(18) }
```

Listing 4: Security metrics related to cryptographic primitives (symmetric and asymmetric encryption), obtained for TelosB.

```
(1) communication {
(2)   medium[wsn] {
(3)     % ...
(4)     topology {
(5)       Sink <- CompromisedSensor;
(6)     }
(7)   }
(8) }
```

Listing 5: Topology for WSN communication channel.

```
(1) communication {
(2)   medium[mgmt] {
(3)     % ...
(4)     topology {
(5)       Attacker -> CompromisedSensor;
(6)     }
(7)   }
(8) }
```

Listing 6: Topology for MGMT communication channel.

for the specific medium (Listing 5). From Listing 5 one can easily deduce that the sink node communicates with both compromised motes (Listing 5, lines (4)–(6)), and attacker exchanges information with compromised devices too (Listing 6, lines (4)–(6)). Article [25] provides a detailed view of the `topology` structure.

4.2. Data Flows and Routing. By specifying the `communication` structure (Listings 5 and 6), it is possible to translate not only the topology of the network, but also packet flows. Defining direction of the arrowheads in the `topology` structure, one is able to map the existing packet flows onto an abstract model and precisely specify the movement of the network traffic. Topology represented in Listing 5 indicates that on a `wsn` channel packets can be send from the sink node to compromised nodes. Concerning `mgmt` communication channel, it is used only by the attacker and compromised nodes (Listing 6). With the help of this channel attacker instructs compromised nodes to flood the base station. Details about the `communication` structure are available in [25].

4.3. OSI Layers and Protocols. Protocol implemented and tested in our scenarios refers to network and transport OSI layers. Designed protocol consists of only one communication step. Its operation is quite simple: compromised nodes, instructed by the attacker, send data messages to sink in order to flood it with useless packets.

4.4. Communication. In listing 7 one can find a definition of the communication structure for one of the communication channels used by the modeled network. Here one can specify a set of parameters, like the quality of the channel (line (4)), default transmission time (line (5)), calculated by the algorithm presented on Listing 9, together with default listening (line (6)), and sending (line (7)) and receiving (line (8)) current values. Details about the algorithm from Listing 9 can be found in [25].

The communication between interconnected devices is modeled by means of channels: sink's ability to store specified number of incoming packets was translated to the size of the buffer given for the specific communication channel (Listing 8). Any type of data can be passed through these channels. Due to the fact that `ch_MGMT(*)` is used only by the attacker to control zombie armies, it acts as the management channel;

```
(1) communication {
(2)
(3)   medium[wsn] {
(4)     default_q = 1;
(5)     default_time = wsn_time [ms];
(6)     default_listening_current = 0.02 mA;
(7)     default_sending_current = 17.4 mA;
(8)     default_receiving_current = 19.7 mA;
(9)
(10)     % ...
(11) }
```

Listing 7: TelosB electric characteristics.

```
(1) channels
(2) {
(3)     channel ch_WSN(192)[wsn];
(4)     channel ch_MGMT(*)[mgmt];
(5) }
```

Listing 8: Utilized communication channels.

there is no limit for message passing by this channel (line (4)). Since in our analysis we focus on volumetric DDoS attacks, which are simply about causing congestion, we needed to model the other channel as a medium with fixed buffer size, to examine its potential overflow. From TelosB datasheet [23] we know that this device is equipped with 48 K bytes of program flash memory, 1024 K bytes of measurement serial flash, and 10 K bytes of RAM. In order to perform our simulations in timely and effective manner, we reduced the message buffer accordingly, in a way that it is capable of storing the maximum of 192 messages and provides asynchronous communication (line (3)). When 192 packets on `ch_WSN` channel are waiting to be processed, its buffer is considered to be full. It means that additional, incoming requests cannot be handled and are, as a result, dropped.

Article [20] contains more information about message passing and the logic of channel's buffer.

5. Multilevel Attack Assessment: Simulation, Results Analysis, and Algorithms

In this section, we describe our simulation environment, mention utilized software, and present detailed results for each of the defined scenarios. In short, the multilevel analysis performed here focuses on many various aspects of the examined problem at once. This means that, during a single analysis, we are able to take into account many different factors at the same time (network architecture and topology, data flows and routing, utilized protocols, and communication and security mechanisms) and examine results in terms of time, energy consumption, financial expenditures, or environmental impact. The metrics utilized here refer to time and energy consumed during the accident, incurred costs (related to the time when the infrastructure could not deliver its services), and the influence on environment.

To examine network performance with different number of compromised, attacking nodes, we implemented 8 scenarios, which are known as *versions* in QoP-ML's nomenclature. Our tests were taken with fully automated tool, designed for the analysis of cryptographic protocols (AQoPA). The selection of the utilized tool was dictated by previous works. In [24, 26, 27], credibility and reliability of the results gathered for internet protocols (TLS, Kerberos) and WSN protocols, modeled with QoP-ML, were carefully inspected and finally verified. Both the model and the AQoPA tool can be downloaded from the web page of the QoP-ML project [1].

5.1. DDoS Attack Evaluation. During analyses performed in this paper, we focused on the percentage of dropped packets in each flood wave and the time taken by the sink to handle incoming packets. Detailed simulation results are presented in Tables 3 and 4.

Gathered results indicate that utilized security mechanisms significantly affect sink's performance. Considering the results obtained for scenarios with packet encryption (scenarios 1, 3, 5, and 7), it is clear that the number of compromised devices has a meaningful impact on DDoS success probability. This relationship is the result of the percentage of dropped packets in each flood wave. As it can be seen from Tables 3 and 4, the more devices the attacker has under his control, the faster the DDoS occurrence. Consider, for instance, scenarios 7 and 8. Here, 50 compromised sensors flood sink with useless messages. With unencrypted traffic, there are any dropped packets (scenario 8). However, when the traffic is encrypted (scenario 7), sink starts dropping packets in 5th flood wave. With 75 compromised sensors, normal network operation is possible until the 5th flood wave for unencrypted traffic and 2nd flood wave for encrypted traffic. When the number of controlled motes increases to 100, distributed denial of service can be observed in 3rd and 2nd flood waves (for unencrypted and encrypted traffic, resp.). The attacker, who has the greatest number of motes (150) under his control, has the most powerful weapon to bring down the whole network; it can cause denial of service generating only 2 flood waves (Figures 2 and 3).

Sink's service time increases with the number of compromised devices as well. Comparing data only for first flood waves in each scenario, one can observe that the time needed by the sink to handle incoming requests extends with the number of motes controlled by the attacker, for both encrypted and unencrypted traffic.

5.2. Multilevel Analysis of DDoS Attack. Besides the performance, we also considered the energy consumed by the sink and estimated its lifetime under the DDoS attack. An interesting conclusion can be drawn from the results of the consumed energy. As it can be seen from Tables 3 and 4, when sink deals with encrypted traffic, it consumes more energy than handling unencrypted packets. It is worth noticing that the number of the flood wave has an impact on the percentage of dropped packets when considering encrypted traffic but

```
(1) algorithms {
(2)     alg wsn_time(msg) {
(3)          msg_size = size(msg[3]);
(4)          xtime = 0;
(5)          while (msg_size > 0) {
(6)               sending = 18;
(7)               one_size = 110;
(8)               if (msg_size < one_size) {
(9)                   one_size = msg_size;
(10)               }
(11)               transmitting = one_size * 0.12;
(12)               xtime = xtime + sending + transmitting;
(13)               msg_size = msg_size - 110;
(14)          }
(15)           return xtime;
(16)     }
(17) }
```

Listing 9: Algorithm used for calculating the packet transmission time in utilized air channels.

Table 3: Detailed simulation results for scenarios 1–4.

Scenario number	Flood wave number	Dropped packets [%]	Time taken by sink to handle incoming packets [s]	Energy consumed by sink [J]	Sink's lifetime [days]
1	1	0	371.45	604.76	21.42
1	2	34	486.79	607.01	21.35
1	3	55	496.61	607.18	21.34
1	4	66	506.43	607.35	21.33
1	5	72	516.24	607.53	21.33
1	6	76	526.06	607.68	21.32
2	1	0	37.68	481.52	26.91
2	2	22	58.15	505.17	25.65
2	3	39	68.14	507.19	25.55
2	4	47	78.13	508.69	25.47
2	5	52	88.13	509.79	25.42
2	6	56	98.12	510.72	25.37
3	1	0	248.74	600.91	21.56
3	2	2	486.79	607.01	21.35
3	3	33	496.61	607.18	21.34
3	4	49	506.43	607.35	21.33
3	5	58	516.24	607.53	21.33
3	6	65	526.06	607.68	21.32
4	1	0	25.49	474.53	27.31
4	2	0	49.86	502.52	25.78
4	3	8	68.14	507.19	25.55
4	4	21	78.13	508.69	25.47
4	5	29	88.13	509.79	25.42
4	6	34	98.12	510.72	25.37

Table 4: Detailed simulation results for scenarios 5–8.

Scenario number	Flood wave number	Dropped packets [%]	Time taken by sink to handle incoming packets [s]	Energy consumed by sink [J]	Sink's lifetime [days]
5	1	0	187.39	599.39	21.62
5	2	0	371.45	604.76	21.42
5	3	11	496.61	607.18	21.34
5	4	32	506.43	607.35	21.33
5	5	44	516.24	607.53	21.33
5	6	53	526.06	607.68	21.32
6	1	0	19.4	445.36	29.1
6	2	0	37.68	481.52	26.91
6	3	0	55.95	494.15	26.22
6	4	0	74.23	500.49	25.89
6	5	5	88.13	509.79	25.42
6	6	12	98.12	510.72	25.37
7	1	0	126.03	589.57	21.98
7	2	0	248.74	600.91	21.56
7	3	0	371.45	604.76	21.42
7	4	0	494.16	606.70	21.36
7	5	16	516.24	607.53	21.33
7	6	29	526.06	607.68	21.32
8	1	0	13.3	454.73	28.5
8	2	0	25.49	474.53	27.31
8	3	0	37.68	481.52	26.91
8	4	0	49.86	502.52	25.78
8	5	0	62.05	501.27	25.85
8	6	0	74.23	500.49	25.89

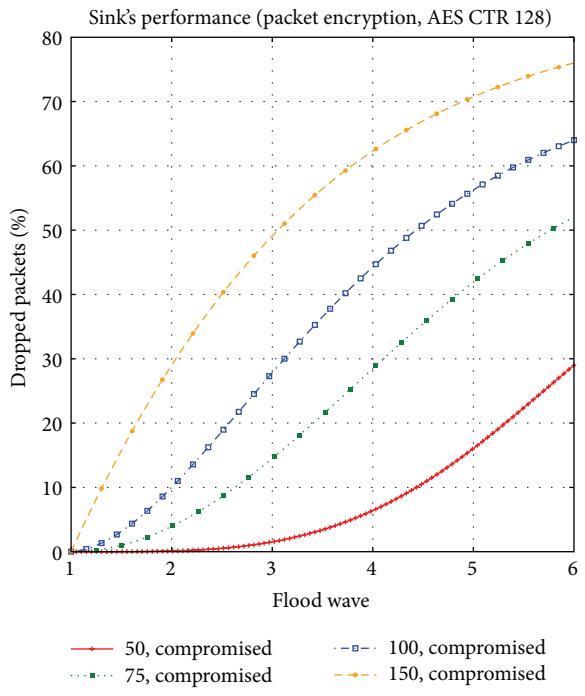

Figure 2: Percentage of dropped packets in each flood wave. Data is encrypted with AES in CTR mode with 128-bit key.

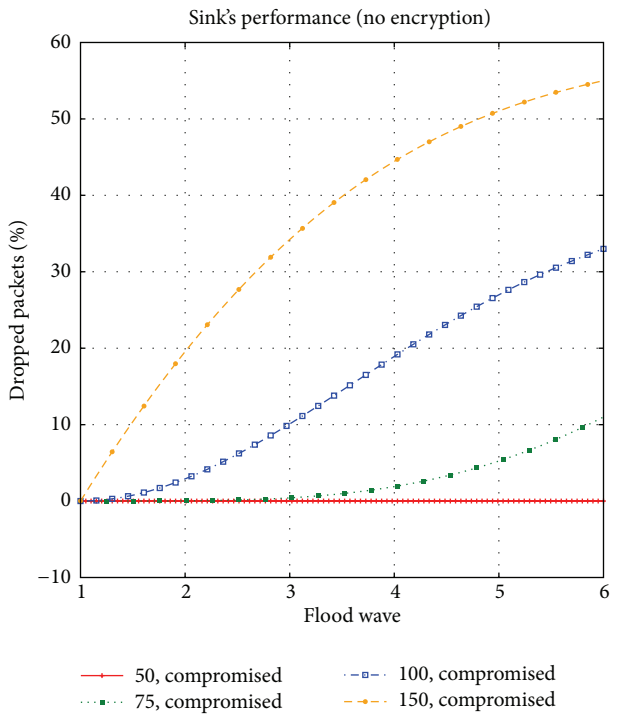

Figure 3: Percentage of dropped packets in each flood wave. Data is unencrypted.

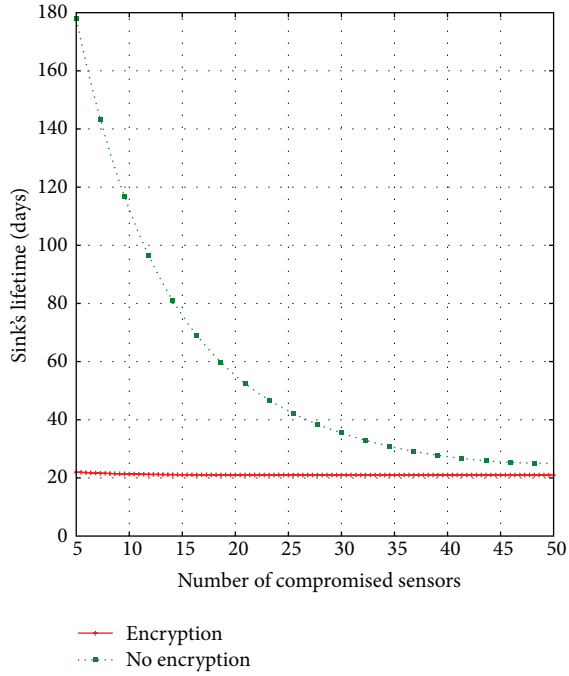

Figure 4: Sink's lifetime for encrypted and unencrypted traffic.

does not affect much the consumed energy. The difference in joules between flood waves in encrypted communication (scenarios 1, 3, 5, and 7) is quite small. Regarding scenarios with nonencrypted data (2, 4, 6, and 8), we presume that it is still possible to bring down the sink, exploiting another aspect of the network, namely, energy resources. Although the gateway copes better with plain packets than encrypted ones when it comes to the number of dropped messages, it fails to resist the attack on energy resources. Obtained results indicate that when compromised sensors continuously flood sink with unencrypted packets, the attack can be undetected by defense mechanisms (because there is no dropped packets) but still can be dangerous, as it reduces the sink's lifetime severely. Consider, for instance, scenario 6, where dropped packets can be observed in 5th flood wave, but the actual attack on energy resources should be noticed and prevented after the first flood wave to stop undesirable resource consumption. To confirm our assumptions, we performed another set of simulations, with less than 50 compromised devices, namely, 5, 10, 15, 20, 25, 30, 35, 40, and 45. We examined the lifetime of the sink node being flooded with useless messages by the mentioned number of sensors with different security mechanisms applied. The influence of DDoS attack on the energy consumed by the sink, which can be further considered as the lifetime prediction, can be observed in Figure 4.

Results available in Figure 4 clearly state that even with unencrypted traffic it is possible to induce a DDoS attack. This special type of DDoS attack is defined by the authors as the DDDoS attack (delayed distributed denial of service). With $5, 10, \ldots, 50$ compromised sensors, for the considered network consisting of 200 devices in total, traditional DDoS defense mechanisms, which relies on the number of dropped packets or the traffic volume, will fail. As it can be seen in Figure 4, if the sink node will be continuously flooded by 5 compromised sensors for 24 hours (by using only the sixth flood wave), its lifetime will be equal to about 21 and 180 days (for encrypted and nonencrypted traffic, resp.). However, when we increase the number of compromised devices to, for instance, 20 sensors, the lifetime of the sink will decrease to about 20 and 55 days (encrypted, nonencrypted). Introduced attack is a nasty kind of distributed denial of service attack, as it can decrease the lifetime of the sink node by slowly and imperceptibly consuming its valuable power, leading to total exhaustion of energy resources. The DDDoS attack is especially dangerous for WSNs, where the energy is one of the constrained resources. In most cases, due to the deployment in remote and hard to access locations, it is very difficult (costly and time-consuming) or even impossible to change the batteries for the sensor nodes. Eliminating the source of an attack is sometimes not enough: when the energy of a sensor reaches a certain threshold, the sensor will become faulty and will not be able to function properly, which will have a major impact on the network performance.

6. Conclusions

In the paper we presented the multilevel analysis of the DDoS attack problem. We defined 8 scenarios with two security levels (encryption/no encryption) and different number of compromised devices (50, 75, 100, and 150). Performing a set of simulations, we investigated the sink's performance and energy consumption under the DDoS attack. By examining the results gathered for prepared simulations, we identified a new kind of distributed denial of service attack, the DDDoS attack. Our analysis showed that although the packets traversing the network are not encrypted (meaning should be less harmful for the sink node in terms of its performance), they still can be dangerous and quietly imperceptibly bring down the whole network, exhausting valuable energy resources.

Another interesting conclusion can be drawn from the above analysis: depending on the type of the DDoS attack, it is possible to adjust the security level in order to prevent different types of attacks. Our simulations showed that, in certain conditions, by lowering security level, it was possible to avoid DDoS or delay its occurrence.

Using the multifaceted analysis approach supported by the Quality of Protection Modeling Language, it was possible to examine the performance of miscellaneous devices, by changing utilized security metrics, and consider gathered results on multiple levels, starting with time and energy consumption, through ecology and finance, ending at quality of protection. Existing frameworks focus on one aspect of an attack at once, while proposed approach is multilevel, thus being capable of examining different characteristics at the same time. The presented DDoS attack model can be further used for testing different attack mitigation methodologies.

Our future work is to focus on DDoS and DDDoS attacks and examine them in detail. We would like to build a scenario, in which we analyze a complex Internet of Things (IoT) network architecture and analyze its performance during the DDoS (and DDDoS) attacks.

Competing Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

References

[1] B. Ksiezopolski, "The official web page of the qop-ml project, 2012".

[2] M. Dhar and R. Singh, "A review of security issues and denial of service attacks in wireless sensor networks," *International Journal of Computer Science and Information Technology Research*, vol. 3, no. 1, pp. 27–33, 2015.

[3] G. Kumar, "Understanding denial of service (dos) attacks using osi reference model," *International Journal of Education and Science Research*, vol. 1, no. 5, 2014.

[4] Isha, A. Malik, and G. Raj, "Dos attacks on tcp/ip layers in wsn," *International Journal of Computer Networks and Communications Security*, vol. 1, no. 2, pp. 40–45, 2013.

[5] A. D. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," in *Handbook of Sensor Networks Compact Wireless and Wired Sensing Systems*, M. Ilyas and I. Mahgoub, Eds., CRC Press, New York, NY, USA, 2004.

[6] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[7] A. Asosheh and N. Ramezani, "A comprehensive taxonomy of DDoS attacks and defense mechanism applying in a smart classification," *WSEAS Transactions on Computers*, vol. 7, no. 4, pp. 281–290, 2008.

[8] D. K. Chaitanya and G. Arindam, "Analysis of denial-of-service attacks on wireless sensor networks using simulation," in *Proceedings of the IT Security for the Next Generation—European Cup*, University of Applied Sciences, Erfurt, Germany, January 2011.

[9] Q. Huang, H. Kobayashi, and B. Liu, "Modeling of distributed denial of service attacks in wireless networks," in *Proceedings of the IEEE Pacific Rim Conference on Communications, Computers and signal Processing*, pp. 41–44, Victoria, Canada, August 2003.

[10] L. Pei, C. Li, R. Hou, Y. Zhang, and H. Ou, "Computer simulation of denial of service attack in military information network using opnet," in *Proceedings of the 3rd International Conference on Multimedia Technology (ICMT '13)*, 2013.

[11] I. Mukhopadhayay, S. Polle, and P. Naskar, "Analysis of denial-of-service attacks on wireless sensor networks using simulation," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 16, 2014.

[12] R. Bhatnagar, "The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network," *International Journal of Computer Science & Engineering Survey*, vol. 3, no. 2, pp. 31–38, 2012.

[13] S. Tripathy and S. Nandi, "Defense against outside attacks in wireless sensor networks," *Computer Communications*, vol. 31, no. 4, pp. 818–826, 2008.

[14] J.-H. Son, H. Luo, and S.-W. Seo, "Denial of service attack-resistant flooding authentication in wireless sensor networks," *Computer Communications*, vol. 33, no. 13, pp. 1531–1542, 2010.

[15] V. S. Dines Kumar and C. Navaneethan, "Protection against denial of service (dos) attacks in wireless sensor networks," *International Journal of Advanced Research in Computer Science & Technology*, vol. 2, no. 1, pp. 439–443, 2014.

[16] L.-C. Chen, T. A. Longstaff, and K. M. Carley, "Characterization of defense mechanisms against distributed denial of service attacks," *Computers and Security*, vol. 23, no. 8, pp. 665–678, 2004.

[17] M. Eian and S. F. Mjølsnes, "The modeling and comparison of wireless network denial of service attacks," in *Proceedings of the 3rd ACM SOSP Workshop on Networking, Systems, and Applications on Mobile Handhelds (MobiHeld '11)*, October 2011.

[18] G. Dini and M. Tiloca, "ASF: an attack simulation framework for wireless sensor networks," in *Proceedings of the IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '12)*, pp. 203–210, Barcelona, Spain, October 2012.

[19] Y.-Y. Zhang, X.-Z. Li, and Y.-A. Liu, "The detection and defence of DoS attack for wireless sensor network," *The Journal of China Universities of Posts and Telecommunications*, vol. 19, no. 2, pp. 52–56, 2012.

[20] B. Ksiezopolski, "QoP-ML: quality of protection modelling language for cryptographic protocols," *Computers & Security*, vol. 31, no. 4, pp. 569–596, 2012.

[21] B. Ksiezopolski, *Multilevel Modeling of Secure Systems in QoP-ML*, CRC Press/Taylor & Francis, New York, NY, USA, 2015.

[22] G. Anastasi, G. Lo Re, and M. Ortolani, "WSNs for structural health monitoring of historical buildings," in *Proceedings of the 2nd Conference on Human System Interactions (HSI '09)*, pp. 574–579, IEEE, Catania, Italy, May 2009.

[23] Crossbow Technology, "TelosB mote platform datasheet," Document Part Number 6020-0094-01, rev B, 2004, http://www.willow.co.uk/TelosB Datasheet.pdf.

[24] I. Mansour, D. Rusinek, G. Chalhoub, P. Lafourcade, and B. Ksiezopolski, "Multihop node authentication mechanisms for wireless sensor networks," in *Ad-Hoc, Mobile, and Wireless Networks: 13th International Conference, ADHOC-NOW 2014, Benidorm, Spain, June 22–27, 2014 Proceedings*, vol. 8487 of *Lecture Notes in Computer Science*, pp. 402–418, Springer, Berlin, Germany, 2014.

[25] D. Rusinek, B. Ksiezopolski, and A. Wierzbicki, "Security trade-off and energy efficiency analysis in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 943475, 17 pages, 2015.

[26] B. Księżopolski, D. Rusinek, and A. Wierzbicki, "On the modelling of kerberos protocol in the quality of protection modelling language (QoP-ML)," *Annales UMCS, Informatica*, vol. 12, no. 4, pp. 69–81, 2012.

[27] P. Szalachowski, B. Ksiezopolski, and Z. Kotulski, "Optimization of the TLS security protocol," *Annales UMCS: Informatica*, vol. 9, pp. 59–75, 2009.