Article

On the Suitability of Intrusion Detection System for Wireless Edge Networks †

Vladimir Shakhov [1,*], Olga Sokolova [2] and Insoo Koo [1,*]

[1] Department of Electrical and Computer Engineering, University of Ulsan, Ulsan 44610, Korea
[2] Institute of Computational Mathematics and Mathematical Geophysics, 630090 Novosibirsk, Russia; olga@rav.sscc.ru
* Correspondence: shakhov@mail.ulsan.ac.kr (V.S.); iskoo@ulsan.ac.kr (I.K.)

† This paper is an extended version of our paper published in 20th International Conference on Computational Science and Its Applications (ICCSA 2020), Cagliari, Italy, 1–4 July 2020; pp. 546–556.

Abstract: Multi-access edge computing has become a strategic concept of the Internet of Things. The edge computing market has reached USD several billion and is growing intensively. In the edge-computing paradigm, most of the data is processed close to, or at the edge of, the network. This greatly reduces the computation and communication load of the network core. Moreover, edge computing provides better support for user privacy. On the other hand, an increase in data processing locations will proportionately increase the attack surface. An edge node can be put out of service easily by being flooded with spoofed packets owing to limited capacities and resources. Furthermore, wireless edge nodes are quite vulnerable to energy exhaustion attacks. In this situation, traditional network security mechanisms cannot be used effectively. Therefore, a tradeoff between security and efficiency is needed. This study considered the requirements under which the use of an intrusion detection system (IDS) is justified. To the best of our knowledge, this is a first attempt to combine IDS quality, system performance degradation due to IDS operations, and workload specificity into a unified quantitative criterion. This paper is an extended version of a report published in the proceedings of the ICCSA 2020 and differs from it in many ways. In particular, this paper considers novel mathematical problems regarding the deployment strategies for an IDS and the corresponding inverse problems and provides closed-form solutions for a few previously unsolved problems.

Keywords: edge computing; IoT devices; wireless communications; flooding attack; energy exhaustion attack; intrusion detection system

Citation: Shakhov, V.; Sokolova, O.; Koo, I. On the Suitability of Intrusion Detection System for Wireless Edge Networks. *Energies* **2021**, *14*, 5954. https://doi.org/10.3390/en14185954

Academic Editor: Massimo Panella

Received: 4 August 2021
Accepted: 15 September 2021
Published: 19 September 2021

1. Introduction

According to an estimate by Cisco Global Cloud Index, the data produced by the Internet of Things (IoT) will soon exceed 800 zettabytes. For efficient treatment of such huge volumes of data, the edge-computing paradigm has been suggested. In this paradigm, most of the data is processed close to, or at the edge of, the network. Some functions of the network core are delegated to the network edges, where the connected entities produce the data directly. The corresponding computing platforms and system resources can fortify these facilities. Edge computing offloads the computation and communication load of the network core, and by processing data near the data sources, it provides a better quality of service (QoS) for delay-sensitive applications and efficient structural support for user privacy, and it prevents and mitigates some types of DDoS attacks [1].

The ratio of enterprise-generated data, which is processed outside of a conventional centralized data center or cloud, is expected to reach 75%. ResearchAndMarkets.com estimates that the total edge computing market will increase to USD 9.0 billion by 2024, at a compound annual growth rate of 26.5%. According to an alternative forecast provided by Gartner, this market will reach USD 13 billion by 2022. Worldwide, the financial industry is one of the largest beneficiaries of edge computing. The increased adoption of digital and mobile banking initiatives, advanced technologies such as blockchain, and payments through smart mobile devices is fueling the demand for modern edge computing solutions. The Asia-Pacific region is destined to become one of the main markets because companies and governmental organizations there show a greater inclination toward storing and processing data locally.

However, an increase in the number of data processing locations will increase the attack surface proportionately [2]. Edge devices are generally used with limited resources [3], and the limited resources of the IoT poses a serious security threat as energy exhaustion and flood attacks, as well as various types of related intrusions have been described [4–9]. In addition, limited computing power and storage size and low battery capacity prevent IoT devices from executing conventional actions to support network security [10]. Storing large amounts of data and executing a highly complex algorithm for intrusion detection are unreasonable. Considering the security challenges, leading academic researchers and experts from for-profit companies concluded that the current situation with IoT and edge computing security is far from satisfactory and essential efforts are required to overcome weaknesses and vulnerabilities. Thus, edge-computing security is rightfully recognized as an important area for future research. [11–13].

A lightweight and secure data analytics technique can increase its potential adoption, which is a major benefit because ensuring that the resource consumption of security systems does not harm the performance of IoT devices is important [14]. Efficiency becomes a crucial issue in secure edge computing, particularly for applications with high real-time requirements. A few recent papers on the theme of intrusion detection systems (IDSs) for edge computing have been published. Some authors offered various IDS mechanisms, but they ignored quantitative analysis [15]. Other researchers focused only on the quality of detection method [16–18], but edge node slowdowns from intrusion detection activities were usually ignored. An edge node usually has extremely limited computational resources and the gateways/endpoints may have the same problem. Hence, it is necessary to take into account the effect of the corresponding additional computational operations. If it is possible to delegate some of the calculations to a central server then heavy ML-based methods like Convolutional Neural Networks, Recurrent Neural Networks can be used. An experimental review of the corresponding methods can be found in [19]. However, we should pay attention to the following circumstance: an intrusion, such as a flood of spoofed requests (packets, tasks) can be very effective against an edge node, regardless of whether the node processes the packet itself or sends it to the cloud.

As shown in a recent survey [20], previous works have mainly focused on the trade-off between IDS performance and resource consumption (energy). There are no quantitative methods in the literature to form a proper holistic view of a defense system and receive requirements for the efficiency of the underlying intrusion detection algorithms. This paper intends to fill this gap partially by describing a novel IDS approach. To the best of our knowledge, this is a first attempt to combine IDS quality, the system performance degradation due to IDS operations, and workload specificity into the unified quantitative criterion.

This paper is an extended version of a report [21] published in the proceedings of the 20th International Conference on Computational Science and Applications (ICCSA 2020, Cagliari, Italy) and differs from it in significant ways. In particular, this paper considers novel mathematical problems concerning the strategies for deploying intrusion detection systems, corresponding inverse problems, and provides closed-form solutions for a few previously unsolved problems.

The remainder of this paper is organized as follows. Section 2 introduces the related concepts in which the types of losses that should rely on an IDS are considered, and the corresponding formalism is provided. Section 3 presents an analysis of IDS deployment applicability using additional assumptions. Section 4 outlines the criteria for IDS deployment on the IoT edge nodes. Section 5 presents the performance analysis, and Section 6 concludes the paper.

2. System Model and Problem Statement

A signature-based intrusion detection approach usually begins with an understanding of the attack patterns, and a detection algorithm is then implemented to find the signatures for the situation in question, assuming that the signature represented the attack accurately. Failing to recognize a new attack is a serious limitation. In contrast, an anomaly-based intrusion detection approach is designed to enable security systems to learn from data without any explicit deterministic rules. The training dataset contains the input samples and the corresponding output. The detection algorithm is trained until the difference between its predicted outputs and real outputs becomes negligible. It is assumed that the trained algorithm can predict intrusions missing from the training dataset. Therefore, the anomaly-based intrusion detection approach applies to a variety of attacks. On the other hand, some detection errors need to be allowed. There is no guarantee that an IDS would be able to protect against all threats even if it were theoretically possible. Even the best intrusion detection algorithm is unlikely to be 100% accurate. Thus, the detection error tolerance is an inherent feature of an IDS. This means that its protection mechanisms are not suitable for all scenarios. Therefore, the deployment of an IDS must be justified for suitability and throughput.

This paper addresses a criterion for IDS deployment on IoT edge nodes and focuses on DDoS attacks such as flooding, which impedes legitimate users and quickly drains the batteries of the mobile edge nodes [4]. An IDS can filter out some of the malicious traffic, but the following losses to legal users are possible.

- A false positive error, known as a false alarm, occurs when an IDS identifies a legal packet as malicious.
- An IDS consumes system resources, which reduces the system throughput, and causes possible packet losses due to buffer overflow.

Therefore, the benefits of using an IDS can be offset by the mentioned losses. Hence, it is necessary to choose a scenario (with or without an IDS) with minimal losses. Figure 1 presents these concepts.

The following two maps can be defined by introducing the corresponding formalism:

$$L_0 : \mathbf{X} \to \mathbf{R}^+ \quad (1)$$

$$L_{IDS} : \mathbf{X} \times \mathbf{Y} \to \mathbf{R}^+ \quad (2)$$

where $\mathbf{X}$ is a set of edge network environmental parameters; the functional $L_0(\mathbf{x}), \mathbf{x} \in \mathbf{X}$ is the loss metrics in the case of the non-use of the IDS; $\mathbf{Y}$ is a set of IDS indicators; and the functional $L_{IDS}(\mathbf{x}, \mathbf{y}), \mathbf{x} \in \mathbf{X}, \mathbf{y} \in \mathbf{Y}$ is the losses metric in the case of IDS deployment.

Thus, the general goal is to solve the following problem:

$$j^* = \arg \max_{j \in \{0\ ,IDS\}} L_j \quad (3)$$

In other words, this paper addressed the following issue: is it advisable to deploy an IDS with given parameters in a given environment?

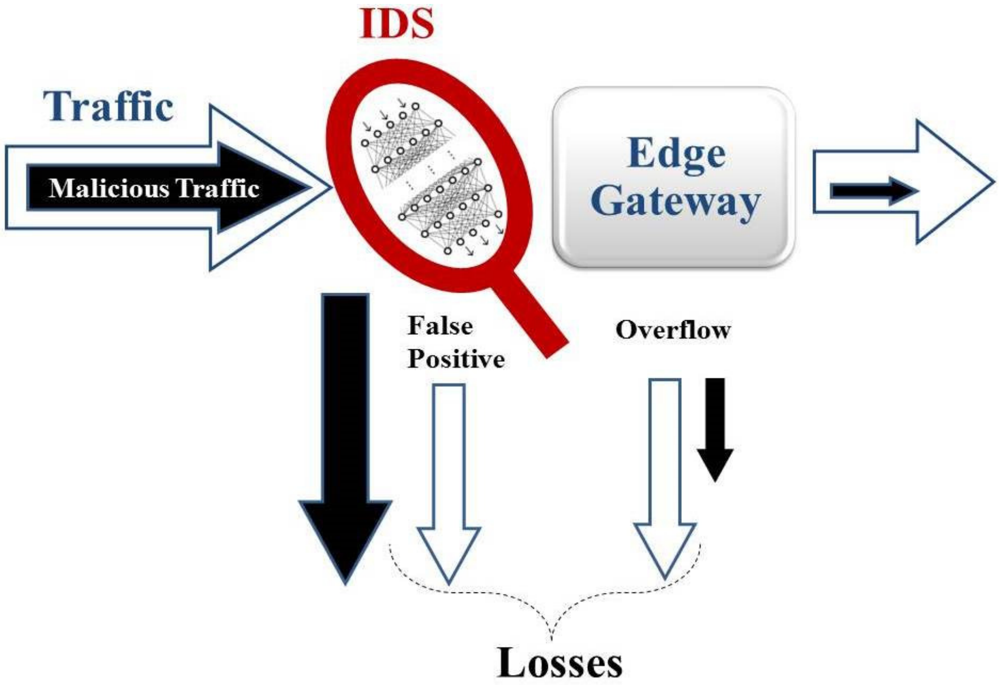

Figure 1. Losses of legitimate users due to the use of an IDS.

This study also considered various problem statements related to (3). For example, if there is an opportunity to affect the environment, then it is reasonable to consider the following problem:

$$\min_{\mathbf{x}\in\mathfrak{Y}} L_0(\mathbf{x}), \mathfrak{Y} \subset \mathbf{X} \tag{4}$$

Here, $\mathfrak{Y}$ is a subset of **X,** depending on resource limits and service-level agreements. An alternative problem can be formulated as follows: This is example 1 of an equation:

$$\min_{\mathbf{x}\in\mathfrak{Y}} f_C(\mathbf{x}) \tag{5}$$

$$\mathfrak{Y} \subset \mathbf{X}$$

$$L_0(\mathbf{x}) \leq \zeta_A$$

where the function $f_C(\mathbf{x})$ describes the cost of recourses used, and ζ_A is the level of admissible losses.

The effective functioning of an IDS entails an increase in resource consumption. Therefore, the overall throughput of the system will be reduced if an IDS is actively used. The problem of IDS deployment is reduced to determining the set:

$$\Omega_x = \{\mathbf{y}| \, (\mathbf{x},\mathbf{y}) \subset \mathbf{X}\times\mathbf{Y}, L_{IDS}(\mathbf{x},\mathbf{y}) < L_0(\mathbf{x})\,\} \tag{6}$$

Taking tight budget constraints for IDS implementation into account, the problem can be formulated as follows:

$$\min_{\mathbf{y}\in\Omega_x} L_{IDS}(\mathbf{x},\mathbf{y}) \tag{7}$$

$$\mathbf{x} \in \mathfrak{Y}$$

$$f_{IDS}(\mathbf{y}) \leq \zeta_{\max}$$

where the function $f_{IDS}(\mathbf{y})$ provides a cost of IDS implementation, and $\zeta_{\max}$ is the maximum allowable cost.

The choice of loss metrics mentioned above can be influenced by the system architecture, the service agreement, the goal of the researcher, the nature of the losses and how they are interpreted by the participants, and the details of the application. If we obtain a convex optimization problem, then the Lagrange multiplier method, which finds the local optima, can be used to find the global minimum of our problem. In general, we deal with non-convex optimization problems (see, for example, [22]); that is, we often need to study the problem of minimizing a loss function over nonconvex sets. Moreover, the domain of a loss function can contain discrete subsets (the number of servers, the memory chip sizes, the number of features used for classification tasks). In these cases, stochastic optimization methods (simulated annealing, swarm algorithms, evolution strategies) can be preferable. Fortunately, in some practical cases, the loss metric is strictly monotonic and continuous. Thus, as will be seen below, a simple consequence of the Weierstrass extreme value theorem allows for the finding the optimal solution and derivation of a criterion, formulated in closed form, for IDS deployment.

Consider some particular implementations of problem (3) using the features typical of wireless communications. In these assumptions, a set of IoT edge nodes serves a user-generated workload. The set includes traffic, which needs to be treated and retransmitted. Let us use the following designations:

- λ: the traffic intensity;
- μ: the intensity of the request treatment;
- α: the percentage of the workload of legal users, which can be estimated using an observable sample or an auxiliary model; and
- B: the probability of packet/request rejection—the blocking probability.

Here, a situation with two types of users is considered. Legitimate users generate traffic with intensity $\lambda\alpha$. Therefore, malicious users generate traffic with the following intensity: $\lambda(1-\alpha)$. Owing to limited resources of edge nodes, a part of the traffic does not receive service and is rejected. Generally, the blocking probability (B) is a function of λ and μ, (the losses rate) is

$$\lambda B(\lambda, \mu), \tag{8}$$

and the served workload rate is

$$\lambda\big(1 - B(\lambda, \mu)\big), \tag{9}$$

Note that not all packets are useful. The actual loss rate of legal users is

$$L_0 = \alpha\lambda B(\lambda, \mu). \tag{10}$$

Consider the edge nodes equipped by an IDS. It is reasonable to assume that part of the malicious requests will be rejected and the novel workload intensity $\tilde{\lambda}$ will be reduced ($\tilde{\lambda} < \lambda$). On the other hand, it does not guarantee that the system throughput will improve. IoT devices need to perform additional operations for intrusion detection, system maintenance, and malicious request filtering. Therefore, the performance of the request treatment needs to be reduced, i.e., the novel intensity of the request treatment becomes $\tilde{\mu}$, and $\tilde{\mu} < \mu$.

A signature-based IDS can be used if the security system is designed to counteract a limited set of known attacks. In this case, the IDS uses a set of rules (signatures) that can detect the presence of an attack pattern. This provides a high level of accuracy for well-known intrusions. A signature-based IDS is usually characterized by low computational cost ($\tilde{\mu} \approx \mu$). The same effect can be reached using a small number of secret bits for requests verification. On the other hand, this situation is not typical for IoT environments. Hands-on experience has shown that attackers often change their hacking tactics and develop new intrusion approaches and instruments. Signature-based detection does not detect slightly modified attacks; much less, it does not detect unknown attacks. Hence, advanced intrusion detection methods must be applied. Furthermore, $\tilde{\mu} \ll \mu$ is not typical for the IoT considering the edge devices level [23]. Low resources render heavy computation algorithms, such as deep learning, ineffective. Therefore, it is reasonable to assume that the performance of a requested treatment did not increase drastically. Moreover, some legitimate requests are mistakenly recognized as illegal and are filtered by an IDS.

The following section examines the cases where IDS deployment makes sense. These cases are formulated, and condition (6) is specified using mathematical modeling.

3. Analysis

3.1. IDS Application

For the purposes of the present study, it is sufficient to consider the IDS parameters as follows:

- p_I is a false positive, the probability of an event when a legitimate request is rejected by the IDS;
- p_{II} is a false negative, the probability of an event when an illegal request is accepted.

Therefore, the IDS rightly rejects the

$$\lambda(1-\alpha)(1-p_{II}), \tag{11}$$

spoofed request per time unit. The loss of legal traffic is

$$\lambda\alpha p_I \tag{12}$$

Hence, the edge nodes need to treat an offered load of intensity:

$$\tilde{\lambda} = \lambda(\alpha(1-p_I) + (1-\alpha)p_{II}). \tag{13}$$

The ratio of legitimate requests has been changed. Now, this ratio is

$$\tilde{\alpha} = \frac{\lambda\alpha(1-p_I)}{\tilde{\lambda}} = \frac{\alpha(1-p_I)}{\alpha(1-p_I) + (1-\alpha)p_{II}} \tag{14}$$

In the case of IDS application, the actual loss rate of legal users is

$$L_{IDS} = \lambda\alpha p_I + \tilde{\alpha}\tilde{\lambda}B(\tilde{\lambda},\tilde{\mu}) \tag{15}$$

The IDS (with the given quality parameters, p_I, p_{II}) is justified if and only if

$$L_{IDS}(p_I, p_{II}) < L_0 \tag{16}$$

Figure 2 illustrate this point. Therefore

$$\alpha\lambda B(\lambda,\mu) - \tilde{\alpha}\tilde{\lambda}B(\tilde{\lambda},\tilde{\mu}) > \alpha\lambda p_I \tag{17}$$

The blocking probability is a non-negative monotonically decreasing function of the variable $\tilde{\mu}$. Hence, the novel intensity of request treatment needs to satisfy the inequality

$$\tilde{\mu} > I\left(\tilde{\lambda}, \frac{\alpha\lambda(B(\lambda,\mu) - p_I)}{\tilde{\alpha}\tilde{\lambda}}\right) \tag{18}$$

where $I(*)$ is the inverse function of $B(*)$.

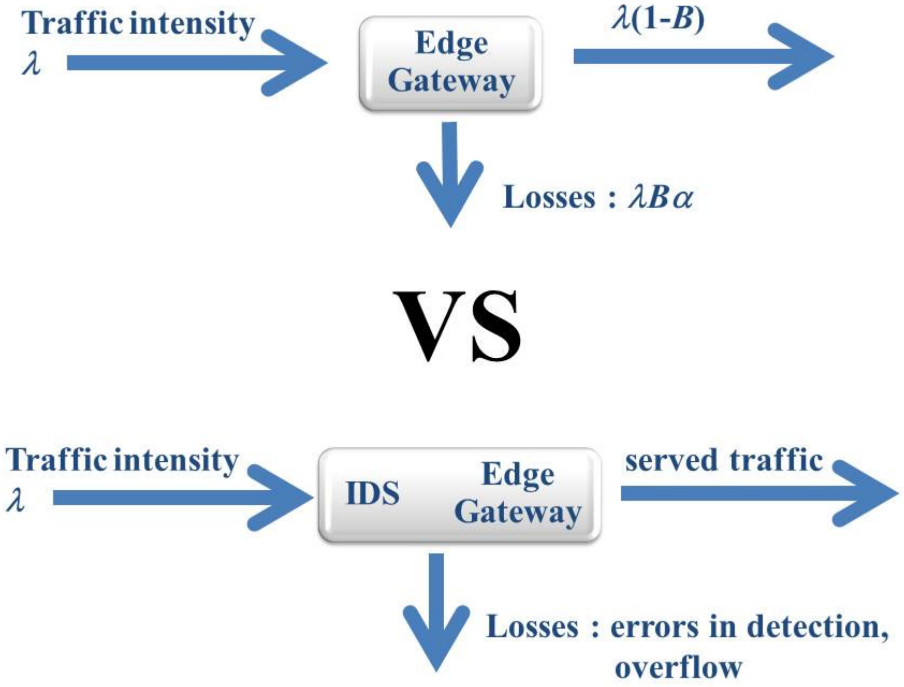

Figure 2. Detailing the problem of choosing an IDS deployment.

In view of the above considerations, inequalities (17) and (18) can be rewritten as follows:

$$B(\tilde{\lambda}, \tilde{\mu}) < \frac{B(\lambda, \mu) - p_I}{1 - p_I} \tag{19}$$

$$\tilde{\mu} > I\left(\lambda(\alpha(1 - p_I - p_{II}) + p_{II}), \frac{B(\lambda, \mu) - p_I}{1 - p_I}\right) \tag{20}$$

These formulae contain only the original system and introduced IDS parameters. The blocking probability function and its inverse can be calculated using an appropriate queuing model. For example, the Erlang-B loss function is perhaps one of the most important mathematical tools that describes the impact of competition for a non-queued limited resource.

3.2. Erlang-B Function

Let us consider a specific model of losses. Taking the requirements of delay-sensitive services into account, it is reasonable to use the M/M/n/n queuing system to model the functioning of the cluster head (gateway), which can serve n requests (e.g., edge devices and sessions) simultaneously. Thus, the assumptions are

- Incoming Poisson flow (with intensity $\tilde{\lambda}$ or λ),
- Exponential service time (with intensity $\tilde{\mu}$ or μ), and
- No buffer (waiting room).

In this case, the blocking probability is described using the Erlang-B formula (see, for example [24]),

$$B(\rho, n) = \left(1 + \Gamma(n+1)\sum_{i=0}^{n} \frac{1}{\rho^{n-i}\Gamma(i+1)}\right)^{-1} \tag{21}$$

where

$$\rho = \frac{\lambda}{\mu} \tag{22}$$

and $\Gamma(n+1)$ is the gamma function.

The inequality (19) can be solved numerically. Please note that the assumption of an exponential cumulative distribution function (CDF) for the service time is unnecessary. The formula (21) is true for M/G/n/n queuing system as well.

Let us consider the case of the equation

$$n \ll \rho \tag{23}$$

which generally takes place under attack. The following theorem [25] was used:

Theorem. *If*

$$\rho \geq n + \tfrac{1}{\varepsilon} \forall\, \varepsilon > 0, \tag{24}$$

then

$$\left\| B(n,\rho) - \left(1 - \tfrac{n}{\rho}\right) \right\| \leq \varepsilon. \tag{25}$$

Corollary. *If ε is small enough, then an approximation for an Erlang-B function can be obtained as*

$$B(n,\rho) \approx 1 - \tfrac{n}{\rho}, \tag{26}$$

and the inverse functions approximations can also be calculated easily

$$\rho \approx \frac{n}{1-B}, \tag{27}$$

$$n \approx \rho(1-B). \tag{28}$$

For heavy workloads, the approximation accuracy reaches machine zero. Therefore, without diminishing the generality, in the consideration below, the entities “approximately equal” and “equal” are identified.

Thus, the M/M/n/n system under a heavy load provides the outgoing rate (served requests) as follows:

$$\lambda\big(1 - B(n,\rho)\big) = \lambda \frac{n}{\rho} = n\mu, \tag{29}$$

and the losses rate is as follows:

$$\lambda B(n,\rho) = \lambda - n\mu \tag{30}$$

3.3. Related Problems

The facts presented in the previous section make it possible to obtain closed-form solutions for a family of problem statements (5). The proposed results can be applied to security issues and various situations, such as placement and resource allocation in mobile edge computing systems, bandwidth minimizing in LoRaWAN, and optimizing the clustering mechanism in VANET. Consider the problem of service differentiation in the term of losses rate, which can arise in situations such as security differentiation for different classes of customers, traffic management, and prioritized time slot assignments performed by V2X protocols. In the case of jamming attacks [26], this technique can be used to assign non-attacked channels to support the survivability of the most critical applications. In general, the problem statement can be formulated as follows. The consumed resources, subject to the required quality of service (limited losses rate) provided, should be minimized as in equation (31):

$$\mathfrak{C}(N) \rightarrow min \tag{31}$$

$$N = \sum_{j=1}^{C} n_j$$

$$B(n_j, \rho_j) \leq b_j, j \in \{1,2,..,C\},$$

where $\mathfrak{C}$ is the function of cost for the consumed resources or energy consumption; N is the total number of computational resources (channels, servers, service centers, IDS agents); C is the number of user classes; n_j is the number of resources assigned to the class *j;* and b_j is the QoS required by class *j* (i.e., the losses rate).

In most cases, minimizing the objective function means minimizing the number of channels, i.e., $\mathfrak{C}(N) \equiv N$. In the case of limited resources (the most critical case), the approximation above helps solve the problem. The optimal solution is as follows:

$$n_j = \rho_j(1 - b_j), j \in \{1,2,..,C\}, \tag{32}$$

and the optimal total number of channels:

$$N^* = \sum_{j=1}^{C} \rho_j(1 - b_j). \tag{33}$$

The theorem in the previous section gives the analytical solution for the following problem of cluster member optimization:

$$M_C \rightarrow max \tag{34}$$

$$B(N, M_C, \lambda_0, \mu) \leq b$$

Where M_C is the number of cluster members; the number of channels N assumed to be fixed; and λ_0 is the intensity of traffic generated by a single cluster member. Remark:

$$\lambda = M_C \lambda_0 \tag{35}$$

The Erlang-B function is a monotonically decreasing function of λ. Hence, the optimal number of cluster members is as follows:

$$M_C^* = \arg\max \{M_C \in \mathbb{N} \mid B(N, M_C, \lambda_0, \mu) = b\} \tag{36}$$

From here

$$M_C^* = \left\lfloor \frac{N\mu}{\lambda_0(1 - b)} \right\rfloor \tag{37}$$

In cognitive radio sensor networks, the set of channels and the set of cluster members are defined in an alternative manner based on link quality metrics and network topology [27]. For these systems, analogically, a solution to the problem of maximizing the permissible traffic intensity for secondary users is

$$\lambda_0^* = \frac{N\mu}{M_C(1 - b)}. \tag{38}$$

4. Criterion

A closed-form solution can be obtained for the inequality (18) in the case of a heavy workload.

Proposition. *The IDS is justified if the following inequality is true:*

$$\tilde{\mu} > \frac{\mu\,(\alpha(1-p_I)+(1-\alpha)\,p_{II})}{1-p_I}. \tag{39}$$

This inequality can be used to estimate and select the intrusion detection algorithms. For convenience, the inequality (39) can be rewritten as a ratio of the request treatment intensities:

$$\frac{\tilde{\mu}}{\mu} > \alpha + \frac{p_{II}(1-\alpha)}{1-p_I} \tag{40}$$

It is often (but not always) expected that a way to improve the false-positive parameter entails the consequences of the proportional degradation of the false-negative parameter and vice versa. This is specific to IDS design. On the other hand, if the IDS quality is good enough, both p_I and p_{II} are small enough. Consider the following ratio:

$$\frac{p_{II}}{1-p_I} \tag{41}$$

If the IDS is of poor quality, the values of p_I and p_{II} will be in the vicinity of 1. Therefore, the ratio becomes large. If the IDS quality is good enough, then the ratio is around zero. Despite some uncertain intermedia cases, the ratio indicates the IDS quality. Thus, let us define the ratio in (41) as the "IDS Performance Index (IDS-PI)". Generally, packets are processed individually by the IDS; hence, this value does not depend on the legal users' packet proportion.

Consider a situation when the efficiency of applied intrusion detection algorithms is very high:

$$\lim_{\substack{p_I \to 0 \\ p_{II} \to 0}} \frac{p_{II}}{1-p_I} = 0 \tag{42}$$

In this case, the criterion for the appropriateness of an IDS takes a simple form:

$$\frac{\tilde{\mu}}{\mu} > \alpha \tag{43}$$

Please note that it is natural to accept that $\tilde{\mu} < \mu$, hence $\tilde{\mu}/\mu \in (\alpha; 1)$.

The decision to deploy an IDS (or provide requirements for one) can be based on profitability analysis. Therefore, a criterion can take a set of various forms, such as "the IDS should improve the loss rate *k* times":

$$\frac{L_{IDS}}{L_0} > k \tag{44}$$

where *k* is a desired constant. In this case, the inequality (18) takes the form

$$\tilde{\mu} > \left(\frac{\lambda}{n} + k\,\left(\mu - \frac{\lambda}{n}\right)\right)\left(\alpha + \frac{p_{II}}{1-p_I}(1-\alpha)\right) \tag{45}$$

An alternative criterion could be: "An effect of IDS implementation is that it has to provide the desired loss threshold *h*":

$$L_{IDS} < h \tag{46}$$

Here, the requirements for system throughput are

$$\tilde{\mu} > \frac{1}{n}\left(\lambda - \frac{h}{\alpha}\right)\left(\alpha + \frac{p_{II}}{1-p_I}(1-\alpha)\right) \tag{47}$$

The approximation above allows a closed-form solution for various similar cases of system profitability analysis. In addition, various solutions can be obtained for inverse problems. For example, if the system performance degradation ($\tilde{\mu}$) due to IDS deployment is given, and it is necessary to define the conditions for one of the other parameters of IDS/environment, then

$$p_I < 1 - \frac{(1-\alpha)\, p_{II}\mu}{\tilde{\mu} - \alpha\mu} \tag{48}$$

$$p_{II} < \left(\frac{\tilde{\mu}}{\mu} - \alpha\right)\frac{1-p_I}{1-\alpha} \tag{49}$$

$$\alpha < \frac{\tilde{\mu}\,(1-p_I) - \ \mu p_{II}}{\mu\,(1-p_I - \ p_{II})} \tag{50}$$

5. Performance Evaluation

In this consideration, it can be assumed that IDS-PI varied in the range (0; 1). Actually, there was no reason for using intrusion detection algorithms with $p_I > 0.5$ or $p_{II} > 0.5$. The following function can be useful for determining the trade-off between the admissible computational overhead and intrusion detection efficiency:

$$g(\alpha, p_I, p_{II}) = \alpha + \frac{p_{II}}{1-p_I}(1-\alpha) \tag{51}$$

The function g provides a critical line separating the acceptable deceleration from the unacceptable one. Figure 3 presents critical lines change according to the IDS throughput efficiency for $\alpha \in \{0.1; 0.3; 0.5; 0.7; 0.9\}$. In accordance with inequality (40), the IDS is justified if

$$\frac{\tilde{\mu}}{\mu} \in \operatorname{epi} g \tag{52}$$

Using this plot, we also obtained the IDS quality requirements.

If the alpha is high enough, the IDS mostly handles legitimate traffic and wastes resources. A small proportion of spoofed packets does not have a significant impact on the network node. In this situation, using such an IDS was justified because it did not slow down the operation of the node and detected almost all spoofed packets. The effect of a mediocre IDS is more like a DDoS attack. It is intuitively clear and shown in Figure 3.

If the portion of legitimate requests is approximately 10 percent, and the IDS leads to a 50 percent decrease in node performance, an IDS-PI of about 0.3 is allowed. This is a very mediocre IDS. In the next example, if the portion of legitimate requests is approximately 90 percent and there is only 15 percent degradation of node throughput, then there are no reasons to use even an ideal ID with no mistakes in algorithm detection (zero false positives and false negatives).

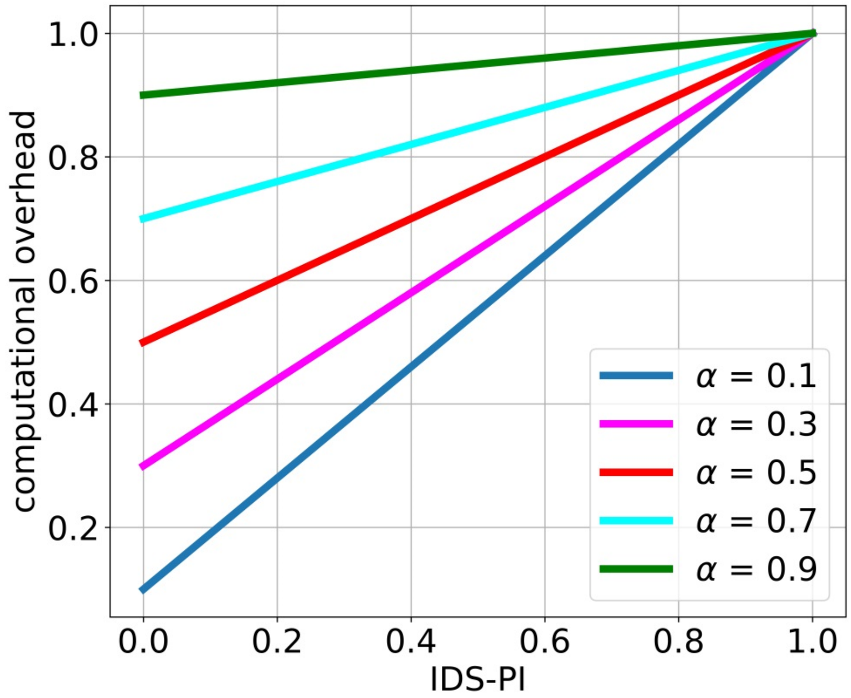

Figure 3. The computational overhead is acceptable if its value lies above the corresponding line.

The suitability of α as a threshold for degradation in node performance was previously noted. Taking into account the inequality (43), we concluded that the throughput of the edge node equipped with IDS could be reduced by less than α^{-1} times; that is,

$$\tilde{\mu} > \mu\alpha \tag{53}$$

This threshold needed to be applied carefully and in a balanced manner. The quality of this approach depends on the quality of the intrusion detection algorithm used. Let us illustrate this proposition. Consider the following value:

$$\text{deviation} = \frac{p_{II}}{1 - p_I}\left(\frac{1}{\alpha} - 1\right) \tag{54}$$

Assume that the false positive and false negative values are small enough. Here, without a loss of generality, $p_I = p_{II} \in \{1\%, 2\%, 3\%, 5\%, 10\%\}$.

If the quality of the intrusion detection algorithm used is very high (the error is approximately one percent or less), then α can be taken as a threshold for reducing the node performance due to the IDS operation. This would not be true if the values p_I and p_{II} exceeded 2 percent, even though this would still be a good enough intrusion detection algorithm. As the quality of intrusion detection algorithms decreases, the second term in formula (51) becomes comparable to α. Figure 4 illustrates this point.

As a final remark, the false positive and false negative values of recently presented energy-efficient IDS reached 5% (see, for example, [28]). Assume that the admissible system performance degradation is limited to 10%. It would be advisable to activate the IDS if the proportion of spoofed packages exceeded 15%; otherwise it would be inappropriate.

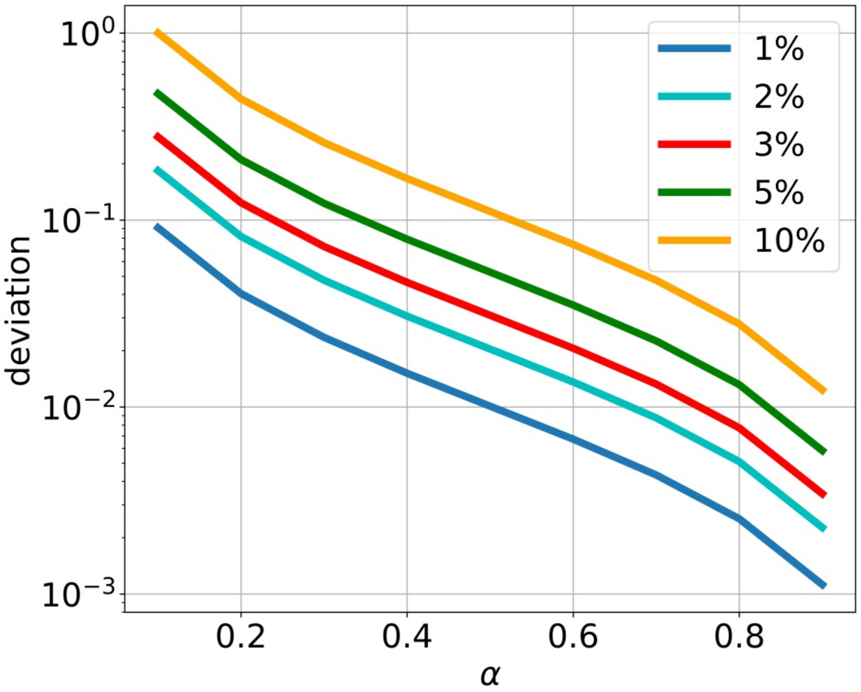

Figure 4. Suitability of α as the node performance degradation threshold.

6. Conclusions

This paper offered a criterion for IDS deployment on IoT edge nodes. The results were based on a queuing theory. In particular, M/M/n/n (M/G/n/n) systems were used. In general, the approach can be applied to any kind of IDS. On the other hand, detailed results were provided for low-resource IoT devices (edge nodes). Using the Erlang losses function approximation, a quantitative condition was received when IDS deployment made sense. The offered approach can mainly be applied for flooding-type intrusions. Note that the result can be used in other application domains, such as enterprises management and hospital operations. In this paper, we provided general tools for analyzing the suitability of an arbitrary IDS. Analyses of specific practical systems will be considered in a future work.

Author Contributions: Conceptualization, V.S., O.S. and I.K.; methodology, V.S., O.S.; software, V.S.; validation, V.S., O.S. and I.K.; formal analysis, V.S.; investigation, V.S., O.S.; resources, V.S., O.S. and I.K.; data curation, V.S.; writing—original draft preparation, V.S.; writing—review and editing, V.S. and I.K.; visualization, V.S.; supervision, V.S. and I.K.; project administration, V.S., O.S. and I.K.; funding acquisition, V.S., O.S. and I.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by a National Research Foundation of Korea (NRF) grant through the Korean Government (MSIT) under Grant NRF-2020R1I1A1A01065692. The research was partially supported by RFBR, project 19-01-00562.

Acknowledgments: We are really grateful to Irina Shakhova for support and providing the valuable and profound comments.

Conflicts of Interest: The authors declare they have no conflicts of interest.

References

1. Zhang, J.; Chen, B.; Zhao, Y.; Cheng, X.; Hu, F. Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. *IEEE Access* **2018**, *6*, 18209–18237.
2. Xiao, Y. Edge Computing Security: State of the Art and Challenges. *Proc. IEEE* **2019**, *107*, 1608–1631.
3. Liu, F.; Tang, G.; Li, Y.; Cai, Z.; Zhang, X.; Zhou, Y. A Survey on Edge Computing Systems and Tools. *Proc. IEEE* **2019**, *107*, 1537–1562.

4. Shakhov, V.; Koo, I. Depletion-of-Battery Attack: Specificity, Modelling and Analysis. *Sensors* **2018**, *18*, 1849.
5. Nguyen, V.-L.; Lin, P.-C.; Hwang, R.-H. Energy Depletion Attacks in Low Power Wireless Networks. *IEEE Access* **2019**, *7*, 51915–51932.
6. Habibzadeh, H.; Nussbaum, B.H.; Anjomshoa, F.; Kantarci, B.; Soyata, T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustain. Cities Soc.* **2019**, *50*, 101660.
7. Desnitsky, V.; Kotenko, I.; Zakoldaev, D. Evaluation of Resource Exhaustion Attacks against Wireless Mobile Devices. *Electronics* **2019**, *8*, 500.
8. Ande, R.; Adebisi, B.; Hammoudeh, M.; Saleem, J. Internet of Things: Evolution and technologies from a security perspective. *Sustain. Cities Soc.* **2020**, *54*, 101728.
9. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of Things for System Integrity: A Comprehensive Survey on Security, Attacks and Countermeasures for Industrial Applications. *Sensors* **2021**, *21*, 3654.
10. Wazid, M.; Das, A.; Shetty, S.; Gope, P.; Rodrigues, J. Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap. *IEEE Access* **2021**, *9*, 4466–4489.
11. Taleb, T.; Samdanis, K.; Mada, B.; Flinck, H.; Dutta, S.; Sabella, D. On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1657–1681.
12. Mao, Y.; You, C.; Zhang, J.; Huang, K.; Letaief, K. A Survey on Mobile Edge Computing: The Communication Perspective. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2322–2358.
13. Porambage, P.; Okwuibe, J.; Liyanage, M.; Ylianttila, M.; Taleb, T. Survey on Multi-Access Edge Computing for Internet of Things Realization. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2961–2991.
14. Bezerra, V.; da Costa, V.; Barbon, S.; Miani, R.; Zarpelão, B. IoTDS: A One-Class Classification Approach to Detect Botnets in Internet of Things Devices. *Sensors* **2019**, *19*, 3188.
15. Yao, H.; Gao, P.; Zhang, P.; Wang, J.; Jiang, C.; Lu, L. Hybrid Intrusion Detection System for Edge-Based IIoT Relying on Machine-Learning-Aided Detection. *IEEE Netw.* **2019**, *33*, 75–81.
16. Lin, F.; Zhou, Y.; An, X.; You, I.; Choo, K. Fair resource allocation in an intrusion-detection system for edge computing: Ensuring the security of Internet of Things devices. *IEEE Consum. Electron. Mag.* **2018**, *7*, 45–50.
17. Garg, U.; Kaushik, V.; Panwar, A.; Gupta, N. Analysis of Machine Learning Algorithms for IoT Botnet. In Proceedings of the 2nd International Conference for Emerging Technology (INCET), Belgaum, India, 21–23 May 2021; pp. 1–4.
18. Ponnusamy, V.; Sharma, B. Investigation on IoT Intrusion Detection in Wireless Environment. In Proceedings of the IEEE International Conference on Computer & Information Sciences (ICCOINS), Kuching, Malaysia, 13–15 July 2021; pp. 7–13.
19. Di Mauro, M.; Galatro, G.; Liotta, A. Experimental Review of Neural-based approaches for Network Intrusion Management. *IEEE Trans. Netw. Serv. Manag.* **2020**, 17, 2480–2495.
20. Pasikhani, A.; Clark, J.; Gope, P.; Alshahrani, A. Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review. *IEEE Sens. J.* **2021**, *21*, 12940–12968.
21. Shakhov, V.; Sokolova, O.; Koo, I. A Criterion for IDS Deployment on IoT Edge Nodes. In Proceedings of the 20th International Conference on Computational Science and Its Applications (ICCSA 2020), Cagliari, Italy, July 1–4 2020; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2020; pp. 546–556.
22. Labana, M.; Hamouda, W. Advances in CRAN Performance Optimization. *IEEE Netw.* **2021**, 35, 140–146.
23. Jan, S.; Ahmed, S.; Shakhov, V.; Koo, I. Toward a Lightweight Intrusion Detection System for the Internet of Things. *IEEE Access* **2019**, *7*, 42450–42471.
24. Harel, A. Sharp and simple bounds for the Erlang delay and loss formulae. *Queueing Syst.* **2010**, *64*, 119–143.
25. Shakhov, V. Simple approximation for Erlang B formula. In Proceedings of the IEEE International Conference on Computational Technologies in Electrical and Electronics Engineering, Irkutsk, Russia, 11–15 July 2010; pp. 220–222.
26. López-Vilos, N.; Valencia-Cordero, C.; Azurdia-Meza, C.; Montejo-Sánchez, S.; Mafra, S.B. Performance Analysis of the IEEE 802.15.4 Protocol for Smart Environments under Jamming Attacks. *Sensors* **2021**, *21*, 4079.
27. Shakhov, V.; Koo, I. An Efficient Clustering Protocol for Cognitive Radio Sensor Networks. *Electronics* **2021**, *10*, 84.
28. Mittal, M.; de Prado, R.P.; Kawai, Y.; Nakajima, S.; Muñoz-Expósito, J.E. Machine Learning Techniques for Energy Efficiency and Anomaly Detection in Hybrid Wireless Sensor Networks. *Energies* **2021**, *14*, 3125.