Modeling the Internet of Things Under Attack: A G-network Approach

Panagiotis Sarigiannidis, *Member, IEEE*, Eirini Karapistoli, *Member, IEEE*, and Anastasios A. Economides, *Senior Member, IEEE*

***Abstract*—This paper introduces a novel, analytic framework for modeling security attacks in Internet of Things (IoT) infrastructures. The devised model is quite generic, and as such, it could flexibly be adapted to various IoT architectures. Its flexibility lies in the underlying theory; it is based on a dynamic G-network, where the positive arrivals denote the data streams that originated from the various data collection networks (e.g., sensor networks), while the negative arrivals denote the security attacks that result in data losses (e.g., jamming attacks). In addition, we take into account the intensity of an attack by considering both light and heavy attacks. The light attack implies simple losses of traffic data, while the heavy attack causes massive data loss. The introduced model is solved subject to the arrival and departure rates in terms of: 1) average number of data packets in the application domain and 2) attack impact (loss rate). A comprehensive verification discussion accompanied by numerous numerical results verify the accuracy of the proposed model. Moreover, the assessment of the presented model highlights notable operation characteristics of the underlying IoT system under light and heavy attacks.**

***Index Terms*—G-networks, Internet of Things (IoT), modeling, queuing theory, security.**

I. Introduction

BUILDING a generic architecture for the Internet of Things (IoT) is a very complex task [1] since there are many layers that have to be considered. The IoT reference model consists of four different layers (device layer, network layer, service support and application support layer, and application layer) engaging a variety of devices, link layer technologies, applications and services. The rationale behind this difficulty lies in the high level of heterogeneity of the inner subsystems of the IoT architecture [2]. Real world IoT deployments are fundamentally heterogeneous, where the coexistence of different types of network technologies, platforms, and protocols poses serious challenges for both academia and industry [3]. In a further aspect, in order to design and apply countermeasures, a robust security modeling is required for mapping and analyzing the potential security and privacy threats against the things, the devices, the applications, and the provided services. From a system perspective, the realization of a complete and secure IoT architecture, together with the required backend network services and devices, still lacks an established best practice because of its novelty and complexity [1]. From a market perspective, the adoption of a clear and secure IoT paradigm is also hindered by the lack of a clear and widely accepted business model that can attract investments to promote the deployment of these technologies [4].

IoT systems will foster the development of new, promising services and applications by utilizing a vast amount of data in open, and often unprotected, areas. In addition, security has emerged as one of the most arduous high-level requirement of IoT deployments. For example, a hospital that is equipped with wireless human body sensors entails a high-quality and a highly insecure IoT system operation. To this end, a precise security system model is of paramount importance in order to effectively monitor the wireless sensors and then take countermeasures upon a security attack takes place.

On the other hand, G-networks have been applied in many communication and networking domains, since they are characterized by flexibility, efficiency, and great scale. For instance, the routing process in communication networks subject to energy efficiency is modeled using a G-network in [5]. The subtle feature of G-networks in this paper is flexibility, since G-networks fit into the routing aspect by formulating the control overhead of the routing process with negative arrivals. In a quite different research field, Xiong *et al.* [6] presented a performance model of OpenFlow networks based on queueing theory. The packet forwarding process of the OpenFlow switches is formulated using simple queueing systems. OpenFlow networks were then analyzed in terms of packet forwarding performance. The authors presented and solved its closed-form expressions of average packet sojourn time and probability density functions. Fourneau and Wolter [7] demonstrated how to model system management tasks, such as load-balancing and delayed download with backoff penalty using G-networks with restart. By placing two or more queues either in parallel or in line, the authors highlight the way of using G-networks in modeling communication network components in an efficient and accurate way.

Manuscript received January 15, 2017; revised May 11, 2017; accepted June 11, 2017. Date of publication June 23, 2017; date of current version December 11, 2017. *(Corresponding author: Panagiotis Sarigiannidis.)*

P. Sarigiannidis is with the Department of Informatics and Telecommunications Engineering, University of Western Macedonia, 50100 Kozani, Greece (e-mail: psarigiannidis@uowm.gr).

E. Karapistoli is with CapriTech Limited, Essex CM17 0ET, U.K.

A. A. Economides is with the Interdepartmental Programme of Postgraduate Studies in Information Systems, University of Macedonia, 54006 Thessaloniki, Greece.

Digital Object Identifier 10.1109/JIOT.2017.2719623

In this paper, we explore the theory of multiplicative networks (also referred to as G-networks) [8] in order to tackle IoT security challenges. G-networks have been used in various applications in modeling computing systems and networks (for example, flow control in computer networks, modeling the effect of viruses in networks, etc.) as well as in solving problems of pattern recognition, combinatorial optimization, etc. [9].

In this paper, we follow the G-network modeling paradigm, and we propose a security threat model in order to achieve comprehensive security management in IoT systems. The proposed model is capable of estimating the data losses in the IoT system with respect to the average number of data streams that the application domain finally receives. In addition, the intensity of the attack is measured in terms of percentage loss in the application domain.

In the light of the aforementioned queueing-based model paradigms, the efficacy of using G-networks for modeling communication models is indicated. These paradigms display the flexibility of queuing theory in applying rigorous models. Thus, the G-network concept is adopted in this paper as the main modeling tool for formulating a generic IoT system. Next, the key contributions of this paper are summarized below.

1) A novel IoT system model is proposed that considers all underlying IoT subsystems, such as the data collection networks, the gateway network, and the application domain. A queueing model is constructed for supporting the operation of such an IoT system. Security attacks are assumed in a generic way, meaning that a variety of different attacks may fit into the introduced model. Furthermore, two attack types are modeled: a) a light attack and b) a heavy attack. The intensity of each attack type is modeled using a simple data packet drop and a batch data stream loss, respectively.
2) A sophisticated queueing network model is proposed for modeling the performance of an IoT system under light/heavy attack. This paper formulates the closed-form expressions subject to the arrival and departure rates, which are considered as known parameters. Furthermore, the average number of data packets that exist in the application domain is calculated. Lastly, the impact of a light and a heavy attack is modeled and solved.
3) A rigorous verification environment is presented indicating the accuracy of the proposed model. Simulation results coincide with the results of the analysis, further confirming the correctness of the presented analysis.

The remainder of this paper is organized as follows. Section II reviews research efforts on designing security models for IoT systems. Section III describes the introduced IoT-enabled security model. In Section V, the proposed analytic model is assessed in multiple simulation experiments and various numerical results are presented and discussed. Finally, Section VI concludes this paper and discusses future extensions.

II. Related Work

The concept of IoT security is not novel. In fact, various official documents consider it as a prime factor that will influence the adoption of the IoT initiative [10]–[12]. More significantly, these documents suggest that as objects, devices and infrastructures in the physical world grow more digitized, the approach to IoT security requires a shift from information technology (IT) security architecture to IoT security architecture [13]. While this shift is central to the IoT security strategy, the current research has not comprehensively investigated how to manage security in IoT in a way different than "traditional" IT security [14].

Current security frameworks for IoT systems mainly include IT-like architectures for providing and managing access control, authentication, and authorization. For example, Ning *et al.* [15] proposed such a system architecture that offers a solution to the broad array of challenges in terms of general system security, network security, and application security with respect to the basic information security requirements of data confidentiality, integrity, availability, authority, nonrepudiation, and privacy preservation. On the other hand, Zhang and Qu [16] proposed a 2-D security architecture integrated with related safety technologies in order to secure IoT systems against possible threats. Riahi *et al.* [17] followed a more holistic design, describing a systemic and cognitive approach for IoT security. In their work, they consider three main axes: 1) effective security for tiny embedded networks; 2) context-aware; and 3) user-centric privacy, and the systemic and cognitive approach for IoT security. Ukil *et al.* [18] considered the embedded device security only, assuming that network security is properly in place, and provide the requirements of embedded security, the solutions to resists different attacks and the technology for resisting temper proofing of the embedded devices by the concept of trusted computing. Some professionals have also considered using radio-frequency identification for further authenticating some of these connected devices [19].

The relation of the IoT domain with the fog/edge computing is presented in [20]. The authors investigate the association of cyber-physical systems and IoT, where existing architectures, enabling technologies and security and privacy issues in IoT are surveyed. This paper includes plenty paradigms and applications of the integration between IoT and fog/edge computing, such as smart grid, smart transportation, and smart cities. Similarly, Yang *et al.* [21] proposed a polynomial-based filtering scheme which can perceive false injected data effectively. The scheme is able to demonstrate a high resilience to the number of compromised nodes without relying on static routes and node localization. This paper studies the replacement of the well-known message authentication codes by the introduced scheme since it allows better authentication process. In particular, each node stores two types of polynomials: 1) authentication polynomial and 2) check polynomial, derived from the primitive polynomial. These elements are used for endorsing and verifying the measurement reports. An application of IoT cyber-physical system in power grid networks was presented in [22]. The authors identify the problem and develop efficient algorithms to identify the optimal meter set.

TABLE I
NOTATIONS AND SYMBOLS

$M = \{M_1, M_2, \cdots, M_N\}$	Number of data collection networks
$\lambda_{0i}^{+},\ i = 1, 2, \cdots, N$	Data packets arrival rate
$\lambda_{0i}^{-},\ i = 1, 2, \cdots, N$	Light security attacks arrival rate
$\mu_i,\ i = 1, 2, \cdots, N$	Data collection network service times
p_{ij}^{+}	Routing probabilities of data packets
p_{ij}^{-}	Routing probabilities of attacks
q_i	Utilization of node i
K_i	Average number of data packets in node i under attack
K_i'	Average number of data packets in node i in a secure IoT

Two defence mechanisms are introduced: 1) a protection-based defence and 2) a detection-based defence. The former one identifies and protects critical sensors and makes the system more resilient to attacks. The latter one develops the spatial-based and temporal-based detection schemes to accurately identify data-injection attacks. A similar approach in [23] studied the vulnerability of the distributed energy routing process. The authors investigated novel false data injection attacks against the energy routing process. Various attack scenarios were explored, in which the adversary may manipulate the quantity of energy supply, the quantity of energy response and the link state of energy transmission.

There are also several research projects funded by various government bodies that directly or indirectly are studying the needs of secure IoT architectures. One of these projects, IoT-A [24], is aiming at providing an architectural reference model for the security of IoT systems. In their model, the authors take into account service privacy and IoT access security aspects throughout the architecture design for dealing with service accommodation, identification, and IoT-A platform realizations.

The major drawback in all above mentioned works is that they have either been designed for certain types of IoT applications or they focus on one aspect of IoT security, and as such, they do not achieve security management in IoT systems as a whole. Contrary to the previous works, in this paper, we explore the theory of G-networks in order to formalize the operation of an IoT architecture and efficiently tackle the security issues that are inherent in this ecosystem. In the subsequent section, we describe the proposed security threat model for IoT systems.

III. SYSTEM MODEL

A. IoT Modeling Under Light Attack

In this paper, an IoT architecture is assumed to consist of $M = \{M_1, M_2, \ldots, M_N\}$ data collection networks, a common infrastructure communication network (i.e., gateway subsystem) in the middle, and an upper application domain. Fig. 1 illustrates the layers of the assumed IoT architecture. Table I summarizes the notations used in our analysis. The set of data collection networks belong to the device layer. The communication infrastructure network define the middle layer between the data collection process and the application domain. A gateway infrastructure forwards the data streams collected in the data collection networks to the upper layer. The application domain aggregates the service support and application support as well as the application layers in a single layer. We formalize the operation of an IoT architecture adopting the G-network theory, which is introduced as an open network that generalizes the Jackson theory in evaluating its performance [25]. As the next generation network paradigm implies, the IoT architecture deals with packet-based data streams that are being carried by the underlying transport infrastructures. In addition, service-related functions are independent from the underlying technologies. Thus, we can infer that the network layer, which is formulated by the gateway subsystem, is based on a packed-based communication fashion between the lower (device layer) and the upper (application layer) layers. Each ordinary customer in the adopted G-network represents a data stream of an average length of *B* bytes. We also consider negative customers in the G-networks representing the security attacks in the IoT system under examination. A negative customer differs from an ordinary (positive) customer in that upon arrival at an IoT subsystem, it kills a positive customer, if any at this subsystem, thereby reducing the number of positive customers at the subsystem by one. As a result the negative customer quits the network receiving no service. Normally, triggers are also considered in a G-network as customers. However, triggers have no use in the context of this paper.

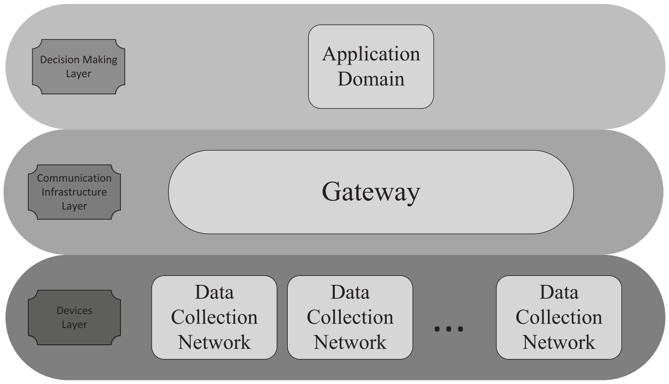

Fig. 1. Layers of the assumed IoT architecture.

The data collection networks feed the gateway subsystem with data streams. Then, the gateway subsystem forwards data streams to the application domain, where they are aggregated and form the application data streams. Thus, the application subsystem consumes the data packets, so they exit successfully the G-network. Normally, a secure IoT architecture is formulated with positive arrivals only. However, in the context of this analysis, we assume both positive and negative arrivals in every data collection network. The positive arrivals denote the data streams that are generated from the IoT devices inside the data collection networks (sensors, actuators, data-capture devices, etc.), while the negative arrivals symbolize security attacks in the data delivery from the data collection networks to the gateway subsystem. In this way, security attacks threatening the data integrity are formulated including denial of service (DoS) attacks, jamming attacks, man-in-the-middle attacks, etc. [26].

Each one of these data collection networks is a single-server with infinitive buffer capacity. Hence, the IoT architecture

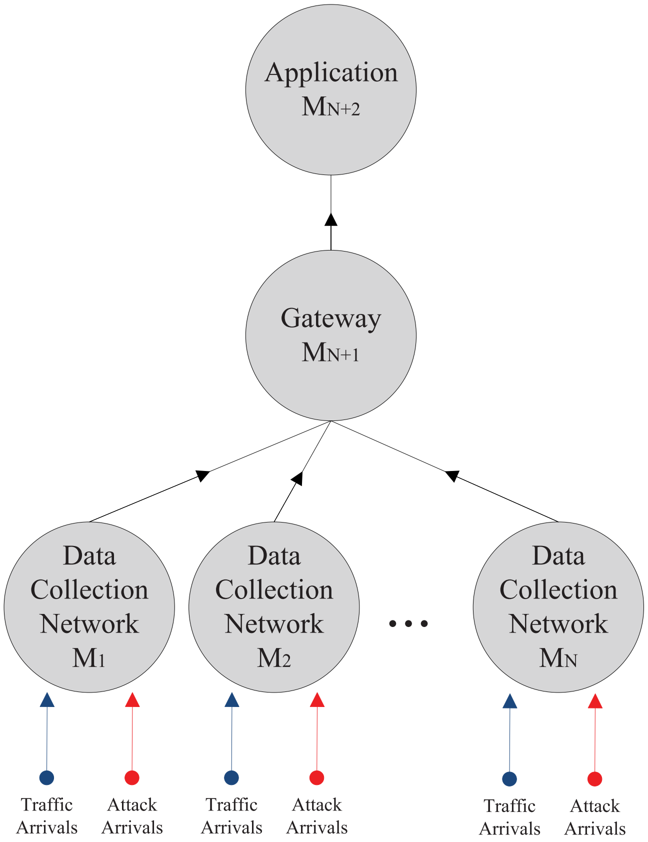

Fig. 2. Cross-layer model approach.

can be formulated by an open G-network with $N + 2$ nodes (subsystems). Every data collection network receives a (Poisson) flow of positive customers (data packets) with rate $\lambda^+_{0,i}$, $i = 1, 2, \dots, N$ and a (Poisson) flow of negative customers (attacks) with rate $\lambda^-_{0,i}$, $i = 1, 2, \dots, N$. Accordingly, a light attack can be seen as a negative customer (a single attack) that kills only a single positive customer (data packet). For example, a short jamming attack in the middle of a wireless sensor network (WSN), which can be represented by the i data collection network, destroys data packets with a rate of $\lambda^-_{0,i}$ data packets per time unit. Fig. 2 show the introduced cross-layer model approach.

In the applied G-network, we define the term "service time" as the routing time from the time a data stream is generated in an IoT device (e.g., sensor node) to the time this data stream is delivered to the IoT gateway (stemming from the sink node of each data collection network). In other words, the service time denotes the routing ability of the data collection network in delivering data packets toward the gateway in the network layer. The service times of the data streams are assumed to be exponentially distributed with parameter μ_i, $i = 1, 2, \dots, N$. It is worth mentioning that the differentiation of the arrival and service times of each data collection network realize the heterogeneity of the underlying IoT system, i.e., every inner data collection network is different in terms of capacity (arrivals) and efficiency (departures); however, all data collections networks are capable of collecting traffic streams and forward them to the IoT gateway.

A light attack in the data collection network implies that data streams are destroyed. As previously mentioned, a negative arrival kills a data packet and then quits the network without receiving any service at the data collection network. As a result, only data streams are delivered by the gateway subsystem.

The gateway acts as a single G-network node. It receives data streams from the N data collection networks and forwards them in the application domain with a service time μ_{N+1}. The service time of the gateway corresponds to the data packet delivery rate of the underlying communication network between the data collection networks and the application upper layer. In essence, it denotes the network throughput of the IoT communication network. Upon their departure at the gateway subsystem, the data streams are considered delivered in the application layer.

The routing probabilities $p^+_{i,j}$ and $p^-_{i,j}$ denote the probability of moving from node i to node j for a data stream and a security attack, respectively. In the light of the aforementioned analysis, the routing probabilities are formed as follows:

$$\begin{aligned} p^+_{0,i} &= 1 \quad \forall i, 1 \le i \le N \\ p^-_{0,i} &= 1 \quad \forall i, 1 \le i \le N && (1) \\ p^+_{0,N+1} &= p^+_{0,N+2} = 0, p^-_{0,N+1} = p^-_{0,N+2} = 0 && (2) \\ p^+_{i,N+1} &= 1, p^-_{i,N+1} = 0 \quad \forall i, 1 \le i \le N && (3) \\ p^+_{N+1,i} &= 0, p^-_{N+1,i} = 0 \quad \forall i, 1 \le i \le N+1 && (4) \\ p^+_{N+1,N+2} &= 1, p^-_{N+1,N+2} = 0 && (5) \\ p^+_{N+2,0} &= 1, p^-_{N+2,0} = 0. && (6) \end{aligned}$$

Let λ^+_i, $\forall i$, $1 \le i \le N+1$, and λ^-_i, $\forall i$, $1 \le i \le N+1$ denote the average arrival rate of the real traffic (data streams) and the attack flows, respectively. The system of nonlinear equations is formed accordingly, where $q_i = (\lambda^+_i / \lambda^-_i + \mu_i)$ stands for the node utilization

$$\lambda^+_i = \lambda^+_{0,i} + \sum_{j=1}^{N+1} q_j \mu_j p^+_{j,i} \tag{7}$$

$$\lambda^-_i = \lambda^-_{0,i} + \sum_{j=1}^{N+1} q_j \mu_j p^-_{j,i}. \tag{8}$$

Lemma 1: Given an IoT system, modeled as a G-network with negative customers, the average arrival rate of the real traffic and the attack flows is given by

$$\lambda^+_i = \lambda^+_{0i}, \lambda^-_i = \lambda^-_{0,i} \quad \forall i, 1 \le i \le N \tag{9}$$

$$\lambda^+_{N+1} = \sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j} + \mu_j} \tag{10}$$

$$\lambda^-_{N+1} = 0 \tag{11}$$

$$\begin{aligned} \lambda^+_{N+2} &= q_{N+1}\mu_{N+1} = \frac{\lambda^+_{N+1}}{\lambda^-_{N+1} + \mu_{N+1}} \mu_{N+1} \\ &= \frac{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j} + \mu_j} \mu_j}{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j} + \mu_j} \mu_j + \mu_{N+1}} \mu_{N+1} && (12) \end{aligned}$$

$$\lambda^-_{N+2} = 0. \tag{13}$$

Proof: Given that the routing probabilities that come from the data collection networks are one way to the gateway node ($p^+_{N+1,i} = p^+_{N+2,i} = p^-_{N+1,i} = p^-_{N+2,i} = 0, \forall i, 1 \leq i \leq N+2$), it holds that

$$\lambda^+_i = \lambda^+_{0,i} + \sum_{j=1}^{N+2} q_j \mu_j p^+_{j,i} = \lambda^+_{0,i} \tag{14}$$

$$\lambda^-_i = \lambda^+_{0,i} + \sum_{j=1}^{N+2} q_j \mu_j p^-_{j,i} = \lambda^-_{0,i}. \tag{15}$$

The average data packet rates in the gateway is calculated as follows:

$$\begin{aligned}\lambda^+_{N+1} &= \sum_{j=1}^{N} q_j \mu_j p^+_{ji} \\ &= q_1\mu_1 + q_2\mu_2 + \cdots + q_N\mu_N \\ &= \sum_{j=1}^{N} q_j\mu_j = \sum_{j=1}^{N} \frac{\lambda^+_j}{\lambda^-_j + \mu_j}\mu_j \\ &= \sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j} + \mu_j}\mu_j. \end{aligned} \tag{16}$$

Since negative customers (security attacks) quit the network ($p^-_{i,N+1} = 0, \forall i, 1 \leq i \leq N+2$) receiving no service upon killing a data stream, the average arrival security attacks in the gateway is zero

$$\lambda^-_{N+1} = 0. \tag{17}$$

In a similar way, the average rates in the application domain are

$$\begin{aligned}\lambda^+_{N+2} &= q_{N+1}\mu_{N+1} \\ &= \frac{\lambda^+_{N+1}}{\lambda^-_{N+1} + \mu_{N+1}}\mu_{N+1} \\ &= \frac{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j}{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j + \mu_{N+1}}\mu_{N+1}. \end{aligned} \tag{18}$$

Since negative customers (security attacks) quit the network ($p^-_{i,N+2} = 0, \forall i, 1 \leq i \leq N+2$) receiving no service upon killing a data packet, the average arrival security attacks in the application domain is again zero

$$\lambda^-_{N+2} = 0. \tag{19}$$

■

Lemma 2: The average number of data packets (capacity) of each one of the $N+2$ nodes of the G-network, denoted as K_i, are given as follows:

$$K_i = \frac{\lambda^+_{0i}}{\lambda^-_{0i} + \mu_i - \lambda^+_{0i}} \quad \forall i, 1 \leq i \leq N \tag{20}$$

$$K_{N+1} = \frac{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j}{\mu_{N+1} - \sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j} \tag{21}$$

$$K_{N+2} = \frac{\frac{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j}{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j+\mu_{N+1}}\mu_{N+1}}{\mu_{N+2} - \frac{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j}{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j+\mu_{N+1}}\mu_{N+1}}. \tag{22}$$

Proof: Given unbounded queue lengths and single-server G-network nodes, it holds that $K_i = (q_i/1 - q_i), \forall i, 1 \leq i \leq N+1$ [5], [27]. Considering the average queue length in the data collection networks, it holds that

$$\begin{aligned}K_i &= \frac{q_i}{1-q_i} \\ &= \frac{\frac{\lambda^+_i}{\lambda^-_i+\mu_i}}{1 - \frac{\lambda^+_i}{\lambda^-_i+\mu_i}} \\ &= \frac{\lambda^+_i}{\lambda^-_i + \mu_i - \lambda^+_i} \\ &= \frac{\lambda^+_{0i}}{\lambda^-_{0i} + \mu_i - \lambda^+_{0i}} \quad \forall i, 1 \leq i \leq N. \end{aligned} \tag{23}$$

■

The average number of data packets is computed in the gateway subsystem as follows:

$$\begin{aligned}K_{N+1} &= \frac{q_{N+1}}{1-q_{N+1}} \\ &= \frac{\frac{\lambda^+_{N+1}}{\lambda^-_{N+1}+\mu_{N+1}}}{1 - \frac{\lambda^+_{N+1}}{\lambda^-_{N+1}+\mu_{N+1}}} \\ &= \frac{\frac{\sum_{j=1}^{N} \frac{\lambda^+_{0j}}{\lambda^-_{0j}+\mu_j}\mu_j}{\sum_{j=1}^{N} \frac{\lambda^+_{0j}}{\lambda^-_{0j}+\mu_j}\mu_j+\mu_{N+1}}}{1 - \frac{\sum_{j=1}^{N} \frac{\lambda^+_{0j}}{\lambda^-_{0j}+\mu_j}\mu_j}{\sum_{j=1}^{N} \frac{\lambda^+_{0j}}{\lambda^-_{0j}+\mu_j}\mu_j+\mu_{N+1}}} \\ &= \frac{\sum_{j=1}^{N} \frac{\lambda^+_{0j}}{\lambda^-_{0j}+\mu_j}\mu_j}{\mu_{N+1}} \end{aligned} \tag{24}$$

$$\begin{aligned}K_{N+1} &= \frac{q_{N+1}}{1-q_{N+1}} \\ &= \frac{\frac{\lambda^+_{N+1}}{\lambda^-_{N+1}+\mu_{N+1}}}{1 - \frac{\lambda^+_{N+1}}{\lambda^-_{N+1}+\mu_{N+1}}}. \end{aligned} \tag{25}$$

By applying $\lambda^-_{N+1} = 0$ in (25), it yields

$$\begin{aligned} K_{N+1} &= \frac{\frac{\lambda^+_{N+1}}{\mu_{N+1}}}{1 - \frac{\lambda^+_{N+1}}{\mu_{N+1}}} \\ &= \frac{\lambda^+_{N+1}}{\mu_{N+1} - \lambda^+_{N+1}} \\ &= \frac{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j}{\mu_{N+1} - \sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j}. \end{aligned} \tag{26}$$

In the same way, the average number of data packets that is finally delivered in the application domain is

$$K_{N+2} = \frac{q_{N+2}}{1 - q_{N+2}} = \frac{\frac{\lambda^+_{N+2}}{\lambda^-_{N+2}+\mu_{N+2}}}{1 - \frac{\lambda^+_{N+2}}{\lambda^-_{N+2}+\mu_{N+2}}}. \tag{27}$$

Given that $\lambda^-_{N+2} = 0$

$$\begin{aligned} K_{N+2} &= \frac{\frac{\lambda^+_{N+2}}{\mu_{N+2}}}{1 - \frac{\lambda^+_{N+2}}{\mu_{N+2}}} \\ &= \frac{\lambda^+_{N+2}}{\mu_{N+2} - \lambda^+_{N+2}} \\ &= \frac{\frac{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j}{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j+\mu_{N+1}}\mu_{N+1}}{\mu_{N+2} - \frac{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j}{\sum_{j=1}^{N} \frac{\lambda^+_{0,j}}{\lambda^-_{0,j}+\mu_j}\mu_j+\mu_{N+1}}\mu_{N+1}}. \end{aligned} \tag{28}$$

B. Attack Impact

In order to model and measure the impact of the attack in the IoT system, we devise the threat impact metric (TIM). TIM measures the intensity of the attack in terms of data packet loss. The metric is recorded in the application layer as the rate of the lost data packets (due to the ongoing attack) to the total data packets delivered in the application domain. Given that (22) expresses the average number of the delivered data packets in the application domain in an IoT under light attack, we define the average delivered data packets, denoted as K'_{N+2}, in an attack-free IoT network, where no negative arrivals exist as follows:

$$K'_{N+2} = \frac{\frac{\sum_{j=1}^{N} \lambda^+_{0,j}}{\sum_{j=1}^{N} \lambda^+_{0,j}+\mu_{N+1}}\mu_{N+1}}{\mu_{N+2} - \frac{\sum_{j=1}^{N} \lambda^+_{0,j}}{\sum_{j=1}^{N} \lambda^+_{0,j}+\mu_{N+1}}\mu_{N+1}}. \tag{29}$$

Then, the TIM is defined as follows:

$$\text{TIM} = \frac{K'_{N+2} - K_{N+2}}{K'_{N+2}}. \tag{30}$$

In essence, TIM measures the average number of the lost data packets caused by the security attack in the data collection networks.

C. IoT Modeling Under Heavy Attack

In this section, we extend the previous model by considering a massive attack in the inner data collection networks of the IoT system. The heavy attack concept may be related to a massive threat, such as a consistent DoS attack or a distributed jamming attack. The main structural model is preserved, thus the IoT system under examination consists of $M = \{M_1, M_2, \ldots, M_N\}$ data collection networks at the left, a common gateway subsystem in the middle (M_{N+1}), and an application domain at the right (M_{N+2}), where the incoming data streams are consumed. Once more, we consider that each data collection network experiences positive and negative customers, denoted as data packet arrivals and (massive) security attacks, respectively. In order to differentiate the intensity of the attack, the batch removal concept is adopted [8]. The batch removal idea defines that a negative customer may kill a batch of positive customers, where the batch size is random and defined by some probability distribution. Assume a node that contains y_i data streams. A negative customer (security attack) arrives at this node. The random variable A_i symbolizes the number of the data packets that a security attack kills upon its arrival at node i. Obviously, if $y_i < A_i$, then the node remains with no data packets at all, and its queue is emptied. Then, the security attack quits that node, without receiving any service. Lastly, A_{max} denotes the maximum number of data packets an attack can kill. The average rates of the real traffic and the attack flows are identical with those in the case of a light attack, that is,

$$\lambda^+_i = \lambda^+_{0i} + \sum_{j=1}^{N+2} q_j \mu_j p^+_{ji} \tag{31}$$

$$\lambda^-_i = \lambda^-_{0i} + \sum_{j=1}^{N+2} q_j \mu_j p^-_{ji}. \tag{32}$$

However, the node utilization is now changed

$$q_i = \frac{\lambda^+_i}{\lambda^-_i f_i(q_i) + \mu_i}. \tag{33}$$

The function $f_i(x)$ stands for the attack intensity in terms of positive customer kills

$$f_i(x) = \frac{1 - \sum_{r=1}^{\infty} A_i x^r}{1 - x}. \tag{34}$$

Given an IoT system under heavy attack, modeled as a G-network with negative customers and batch removal, the average arrival rate of the real traffic and the attack flows is

$$\lambda^+_i = \lambda^+_{0i}, \lambda^-_i = \lambda^-_{0i} \quad \forall i, 1 \le i \le N \tag{35}$$

$$\lambda^+_{N+1} = \sum_{j=1}^{N} q_j \mu_j \tag{36}$$

$$\lambda^-_{N+1} = \sum_{j=1}^{N} q_j \mu_j \tag{37}$$

$$\lambda_{N+2}^{+} = q_{N+1}\mu_{N+1} \tag{38}$$

$$\lambda_{N+2}^{-} = q_{N+1}\mu_{N+1}. \tag{39}$$

By observing (36) to (39), it is clear that a nonlinear system of equations exists; hence, it is difficult to express it further subject to the average arrival rates of the data collection networks. In a similar way, the average number of the data packets in each one of the $N+2$ IoT nodes is expressed in a generic form

$$K_i = \frac{q_i}{1-q_i}. \tag{40}$$

Lemma 3: Given a fixed random variable $P[A_i = B] = 1$, the solution of q_i, denoted as $s_i, 0 < s_i < 1$, where $q_i, \forall 1 \leq i \leq N$, stems from the third-degree equation: $F(q_i) = \mu_i q_i^3 - (2\mu_i + (B+1)\lambda_{0i}^{-} + \lambda_{0i}^{+})q_i^2 + (\mu_i + \lambda_{0i}^{-} + 2\lambda_{0i}^{+})q_i - \lambda_{0i}^{+} = 0$.

Proof: If we apply $P[A_i = B] = 1$ to (34), it yields

$$f_i(x) = \frac{1 - \sum_{r=1}^{\infty} Bx^r}{1-x} = \frac{1 - B\sum_{r=1}^{\infty} x^r}{1-x}. \tag{41}$$

Given that $\sum_{r=1}^{\infty} x^r = (x/1-x)$, (41) becomes

$$f_i(x) = \frac{1 - B\frac{x}{1-x}}{1-x} = \frac{1-x-Bx}{(1-x)^2}. \tag{42}$$

Equation (33) now becomes

$$q_i = \frac{\lambda_i^{+}}{\lambda_i^{-}\frac{1-q_i-Bq_i}{(1-q_i)^2} + \mu_i} \quad \forall 1 \leq i \leq N. \tag{43}$$

Further, by applying (35), it yields

$$q_i = \frac{\lambda_{0i}^{+}}{\lambda_{0i}^{-}\frac{1-q_i-Bq_i}{(1-q_i)^2} + \mu_i} \quad \forall 1 \leq i \leq N. \tag{44}$$

Equation (44) is solved subject to q_i

$$\begin{aligned} \lambda_{0i}^{+}(1-q_i)^2 &= \lambda_{0i}^{-}\Big(q_i - q_i^2(B+1)\Big) + \mu_i q_i (1-q_i)^2 \\ &\Rightarrow \mu_i q_i^3 - \big(2\mu_i + (B+1)\lambda_{0i}^{-} + \lambda_{0i}^{+}\big)q_i^2 \\ &\quad + \big(\mu_i + \lambda_{0i}^{-} + 2\lambda_i^{+}\big)q_i - \lambda_{0i}^{+} \\ &= 0 \end{aligned} \tag{45}$$

The solution of (45) is $q_i = s_i$, where $0 < s_i < 1$ in order to ensure the stability of each i data collection node. ■

It is now easy to define the average number of data packets in the gateway

$$\begin{aligned} K_{N+1} &= \frac{q_{N+1}}{1-q_{N+1}} \\ &= \frac{\frac{\lambda_{N+1}^{+}}{\mu_{N+1}}}{1 - \frac{\lambda_{N+1}^{+}}{\mu_{N+1}}} \\ &= \frac{\lambda_{N+1}^{+}}{\mu_{N+1} - \lambda_{N+1}^{+}} \\ &= \frac{\sum_{j=1}^{N} s_j \mu_j}{\mu_{N+1} - \sum_{j=1}^{N} s_j \mu_j}. \end{aligned} \tag{46}$$

Similarly, the average number of data packets in the application domain is given by

$$\begin{aligned} K_{N+2} &= \frac{q_{N+2}}{1-q_{N+2}} \\ &= \frac{\frac{\lambda_{N+2}^{+}}{\mu_{N+2}}}{1 - \frac{\lambda_{N+2}^{+}}{\mu_{N+2}}} \\ &= \frac{\lambda_{N+2}^{+}}{\mu_{N+2} - \lambda_{N+2}^{+}} \\ &= \frac{q_{N+1}\mu_{N+1}}{\mu_{N+2} - q_{N+1}\mu_{N+1}} \\ &= \frac{\lambda_{N+1}^{+}}{\mu_{N+2} - \lambda_{N+1}^{+}} \\ &= \frac{\sum_{j=1}^{N} s_j}{\mu_{N+2} - \sum_{j=1}^{N} s_j}. \end{aligned} \tag{47}$$

Finally, TIM is defined by combining (29) and (47)

$$\text{TIM} = \frac{K'_{N+2} - K_{N+2}}{K'_{N+2}}. \tag{48}$$

IV. Practical Exploitation

The focus of this section is twofold. First we study possible practical exploitation opportunities of the proposed model in various security domains. Second we discuss potential expansion of the proposed model in practical IoT application domains.

In the context of exploiting our model in different security domains, the most important threats in the IoT domain are examined in terms of intensity, detection criteria, and applicability. The intensity expresses the level of the ongoing attack, i.e., light or heavy. The detection criteria define the way of exposing an attack based on the proposed model, i.e., the TIM metric. Lastly, the applicability indicates the ability of the proposed model to perceive the ongoing attack in IoT domains. Eight total attack forms are investigated, namely the DoS and the jamming attack, the distributed DoS (DDoS) attack, the physical damage, the node capture and controlling, the Sybil attack, the eavesdropping, the sinkhole attack, and the wormhole attack. Table II summarizes the impact comparison subject to different kind of attacks.

A DoS attack occurs when the IoT infrastructure is flooded with useless traffic flows by an external attacker resulting in resource exhaustion, service termination and IoT application unavailability [28]. Normally, DoS falls in the light attack category. However, if the DoS attacks occurs in multiple domains of the underlying data collection networks of the IoT infrastructure then it is deemed as a DDoS attack and its density is high. The proposed model may expose a DoS attack by measuring the data losses (TIM) in the devices layer and the communication infrastructure layer as well. In the case of a DDoS attack the recorded data losses will be higher and the occurred unavailable services due to the attack will be also more intense. The model will monitor the application layer for losses and application/service denial. The applicability of the proposed model in these two forms of attack is high.

TABLE II
MODEL EXPLOITATION IN DIFFERENT ATTACK FORMS

Form of Attack	Intensity	Detection Criteria	Applicability
DoS and jamming	Light	TIM	High
DDoS	Heavy	TIM and service termination	High
Physical damage	Light	Implicit TIM	Medium
Node capture and controlling	Light	Implicit TIM	Medium
Sybil Attack	Light	Implicit TIM	Low
Eavesdropping	N/A	N/A	N/A
Sinkhole	Light	TIM	High
Wormhole	Light	TIM	High

Physical damage is a kind of attack that can be considered as a subcategory of the DoS attack. External attackers may harm the provisioning of IoT services by capturing, destroying or even physically hindering the IoT devices, sensors and actuators. This is a realistic attack in the IoT context, because things might be easily accessible to anyone (e.g., a street light) [29]. These physical damages will implicitly cause data losses. Hence, the model will perceive the anomaly by observing the average number of packet loss either in the gateway or in the application domain. However, the applicability of the introduced model regarding physical damages is medium since the anomaly detection comes through implicit observations. Node capture and device controlling fall in the same category as the physical damage.

In a Sybil attack, a single node presents multiple identities to other nodes in the network [30]. Usually Sybil attacks pose a significant threat to routing protocols by reducing the effectiveness of multipath routing, fault-tolerant schemes, and topology building. As a result, alternative routing paths will not be available in case of emergency. In addition, the implications of the attack in the routing performance may result in data losses. Thus, this type of attack may be detected by measuring the TIM metric in the gateway subsystem. Nonetheless, the model will be able to detect a Sybil attack, if the attacker causes data losses due to routing or other implications. Otherwise, the presented model is not able to perceive any kind of threat in the IoT infrastructure.

Eavesdropping is another popular attack in wireless networks, WSNs and communication networks. External attackers “listen” to communication channels in order to extract information between the data collection networks and the gateway. Due to the passive nature of this attack the implications in the IoT infrastructure are low but hard to be detected. As a result the proposed framework seems unable to expose such a passive attack.

On the other hand, sinkhole and wormhole attacks are related with the data collection network domain, where the main data gathering takes place. Both cause complications in delivering information from the IoT devices to the upper layers. Sinkhole may create a “black” hole inside the data collection network, where critical information is dropped. Similarly, a wormhole link creates a “bad” communication link which causes packet drops since this link is not a working communication path. In both cases, the result is demonstrated by observing the data losses in specific data collection networks. Hence, the TIM metric is capable of reporting such kind of attacks since IoT applications in the upper layer will be underutilized. The proposed model can be quite helpful in detecting sinkhole, wormhole, and even other similar attacks, such as the selective forwarding attack.

TABLE III
MODEL IMPACT IN IoT APPLICATION DOMAINS

Application Domain	Impact
Smart Grid	Confidentiality of energy consumption information
Smart Transportation	Integrity of vehicle networks data
Smart Cities	Protection of smart applications and services (waste and metering management)

In the context of possible expansion of our model in practical IoT application domains, we discuss the most important IoT applications, such as smart grid, smart transportation, and smart cities subject to potential functioning of the model presented in this paper. Table III summarizes the potential impact of the proposed model in the most important IoT domains. Smart grids consist of a large number of smart meters. Smart meters are realized as IP-based IoT devices which communicate with each other via wireless communication links. External attackers can easily capture these smart meters, nodes in fog/edge computing infrastructure, and obtain or modify the data collected [20]. The proposed model is able to contribute to detecting such attacks by measuring and analyzing the data losses in the upper layers.

Another significant IoT paradigm is smart transportation. The evolution of IoT leads to the emergence of Internet of vehicles which is an IoT domain of paramount importance [31]. Intelligent transportation management, control system, communication networks, and computing techniques are integrated to make transportation systems reliable, efficient, and secure [32]. Mobile things, e.g., drones and IP-based vehicles exchange traffic flows each other for processing all that information in order to make intelligent decisions, e.g., optimal path determination. However, these systems seem to be vulnerable to adversaries, where malicious attacks may cause traffic information loss and misleading information sharing. Our scheme could contribute to protect the confidentiality and the integrity of the exchanged information by applying an efficient detection mechanism in the underlying IoT transportation infrastructure.

Smart cities can be considered a complex IoT paradigm which enables a set of compelling smart services and applications giving emphasis in public resource management (e.g., energy and water), reduction of operational public costs and efficient public administration [1]. All supported application and services behind the smart cities paradigm should be protected by security detection mechanisms in a cross-layer approach. For instance, a smart metering IoT system that is focused on measuring the energy consumed in smart houses should be secured in the device layer (data collection networks), the gateway layer (network communication links), and in the application layer (smart phone application) [33]. The proposed IoT model could establish a large-scale secured interconnected heterogeneous network for IoT smart city applications, where distributed anomaly detection frameworks could effectively identify potential threats in the whole IoT system.

V. Verification and Numerical Results

This section presents the evaluation environment and the numerical results of the conducted simulation experiments.

A. Verification Environment

A verification environment was design to assess and evaluate the proposed security model. A generic IoT infrastructure was considered as a simulation basis for applying various types of attacks. The adopted generic IoT infrastructure could realize a wide range of real testbeds. For example, the constrained IoT (CIoT) could be adopted as the main IoT infrastructure [34], where CIoT nodes are connected at the physical layer by IEEE 802.15.4 wireless links, whereas IPv6 is used at the network layer in combination with IPv6 over low-power wireless personal area network (6LoWPAN) and the routing protocol for low-power and lossy networks. The underlying operating system could be the Contiki while each node is equipped with a TelosB interface. The constrained application protocol (CoAP) is used in the application layer. CoAP is a specialized Web transfer protocol for use with CIoT nodes. Another option is message queuing telemetry transfer protocol that runs in the upper levels of the adopted CIoT infrastructure. In any case, it is important to point that the introduced IoT system model of this paper is suitable for a wide range of IoT applications since it expresses the behavior of an IoT network under attack independently of the exact attack form and the strict hardware and software interfaces of the IoT system.

To this end, we developed an IoT-based simulation environment in MATLAB. An IoT system was implemented consisting of N data collection networks, a gateway layer (node $N+1$), and an application domain (node $N+2$) that eventually receives the data streams originated among the connected data collection edges. The data collection networks consist of nodes that are connected at the physical layer by IEEE 802.15.4 wireless links. Each data collection network is directly connected to the gateway node. The gateway node runs at the network layer in combination with the 6LoWPAN protocol. Data streams from the data collection nodes are forwarded to the gateway. The gateway receives the data streams from the data collection networks and then forwards these streams to the application domain. CoAP protocol is used for providing Web transfer services and connecting CIoT with the lower network layers. The performance of the underlying IoT system is related to the application domain efficiency, since the application consumes the data streams coming from the IoT edges.

Each data collection network receives data stream with a Poisson arrival rate equal to $\lambda^{+}_{0,i}$, $1 \leq i \leq N$. Furthermore, each data collection network, as well as the gateway and the application domain, forward data streams with a departure rate of μ_i, $1 \leq i \leq N+2$. Rate μ_{N+1} denotes the delivery ratio of the gateway node, i.e., its throughput. On the other hand, rate μ_{N+2} stands for the consuming rate of the application domain. Data streams are consumed by the application node, and then, they are exported from the IoT network.

Two attack types were considered in the verification environment: a light attack and a heavy attack. The light attack mode corresponds to a simple IoT threat that targets the data stream integrity. A light attack can be realized by a DoS or a jamming attack in the IEEE 802.15.4 wireless links, wormhole or sinkhole attacks in the underlying WSN domains and a physical damage in one or more CIoT devices. In our case, we consider a light attack, as a jamming attack, in a WSN that is represented by the data collection network in our simulation environment. A constant jammer repeatedly emits a radio signal in data collection domains. As a result the constant jammer can effectively prevent legitimate traffic sources from transferring data streams to the upper network layers. The intensity of the attack is measured based on the $\lambda^{-}_{0,i}$, $1 \leq i \leq N$ arrivals in the data collection networks. A heavy attack instead, corresponds to a distributed attack that may happen in multiple domains in a simple data collection network, e.g., a DDoS attack. The heavy attack causes multiple data stream losses. Each heavy attack acts with a rate of $\lambda^{-}_{0,i}$, $1 \leq i \leq N$. As a result, a group of B data streams are lost for each negative arrival of a heavy attack action.

B. Performance Metrics

The performance evaluation as well as the verification of the analytic equations are presented in terms of two performance metrics: 1) the average number of data streams in the application domain and 2) the TIM parameter, as defined in Section III-B. Moreover, in each presented case, the stability of each of the IoT nodes is respected, i.e., the utilization of each of the $N+2$ nodes (q_i) has to be within (0, 1).

The results of the conducted experiments are presented in three forms. First, the average number of data streams in the application domain is presented. In each of these figures, three curves are plotted, namely the secure IoT, the lightly attacked IoT, and the heavily attacked IoT. Secure IoT implies an IoT system without any threat being in place. In the lightly attacked scenario, the IoT is under a light attack, meaning that each of the data collection networks are being attacked by a light attack as described in Section III-A. Accordingly, the heavily attacked IoT curve corresponds to the heavy attack model as analyzed in Section III-C. In the second form, TIM parameter is plotted in highlighting the attack impact in terms of data streams losses. The corresponding figures present the results of the conducted experiments in two curves. The former one expresses TIM under light attack, while the latter one plots TIM under heavy attack. The last form is used to provide evidences about the accuracy of the presented analysis. For each one of the conducted experiments a table summarizes the error of the analysis in terms of absolute difference between the analytic and the simulated values.

C. Data Collection Networks Impact

In this section, the results of the conducted experiments are presented as a function of the number of the data collection networks (N). N ranges from 1 to 20, while the arrival and

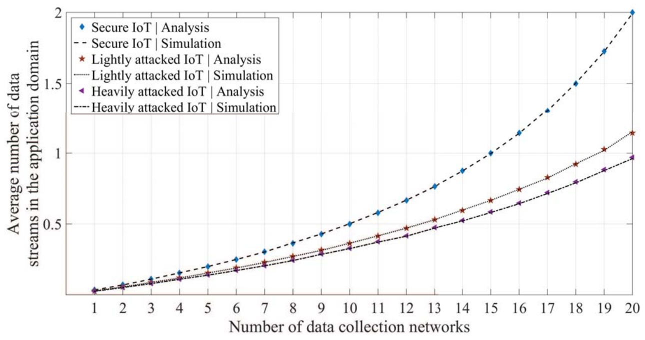

Fig. 3. Average number of data streams in the application domain as the number of the data collection networks is changed.

the departure rates as well as the batch level are kept stable. In particular, the arrival rate in each data collection network is identical and equal to 1 data stream per time unit. The arrival rate of the security attacks is 0.5 data streams per time unit, keeping an 2 : 1 ratio regarding the positive to negative arrivals. Finally, the departure rate of each data collection network is 2 data streams per time unit so as to ensure the stability of the IoT system. Accordingly, the utilization of each data collection network becomes

$$q_i = \frac{\lambda_{0,i}^+}{\lambda_{0,i}^- + \mu_i} = \frac{1}{0.5 + 2} = 0.4 < 1. \tag{49}$$

In addition, the gateway delivery rate was set to 20 data streams per time unit in order to ensure the stability of the gateway node. Thus, the gateway utilization becomes

$$q_{N+1} = \frac{\lambda_{N+1}^+}{\mu_{N+1}} = \lambda_{N+1}^+ = \frac{\sum_{j=1}^{N} \frac{\lambda_{0,j}^+}{\lambda_{0,j}^- + \mu_j}\mu_j}{\mu_{N+1}}. \tag{50}$$

When the number of data collection networks is minimum, i.e., 1, the gateway utilization becomes 0.04, while in the case of a maximum number of data collection networks it yields 0.8. Hence, in both cases the stability of the gateway node is ensured. In a similar way, the application consuming (departure) rate is kept 30 yielding a ratio of 2 : 3 regarding the ratio of the gateway to the application domain. Lastly, the batch level is fixed and equal to 5. That results to a loss of 5 data streams upon a negative arrival in each data collection network assuming the heavily attacked IoT scenario.

Fig. 3 shows the average number of data streams in the application domain as the number of the data collection networks is changed from 1 to 20. By observing the progress of the three curves in the figure, it is easy to infer that the impact of both attacks is significant. In particular, the impact is progressively getting larger as the number of the data collection networks are increased. This is expected due to the fact that as the number of the data collection networks becomes larger, the data stream losses are getting larger as well, since more attacks take place. It is worth mentioning that about 0.8 less data streams appear in a light attack compared to the secure IoT case. The situation is escalated in the case of the heavy attack, where the delivered data streams are even less (reduced at 1).

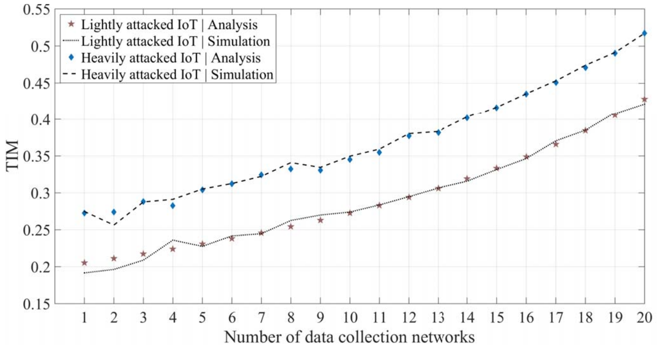

Fig. 4. TIM values as the number of the data collection networks is changed.

TABLE IV
DIFFERENCE ERROR BETWEEN THE ANALYSIS AND SIMULATION AS THE NUMBER OF DATA COLLECTION NETWORKS IS CHANGED

$\cdot\mathbf{10^{-4}}$	**absolute difference** vs number of data collection networks (1-20)									
Secure IoT	1	2	3	4	5	6	7	8	9	10
	0	**19**	**4**	**14**	**3**	**6**	**18**	**37**	**11**	**20**
	11	12	13	14	15	16	17	18	19	20
	23	**14**	**2**	**5**	**21**	**28**	**12**	**46**	**20**	**69**
Lightly attacked IoT	1	2	3	4	5	6	7	8	9	10
	5	**5**	**6**	**8**	**4**	**14**	**10**	**3**	**21**	**7**
	11	12	13	14	15	16	17	18	19	20
	13	**5**	**4**	**25**	**4**	**8**	**53**	**22**	**73**	**62**
Heavily attacked IoT	1	2	3	4	5	6	7	8	9	10
	1	**2**	**4**	**5**	**12**	**16**	**10**	**12**	**21**	**20**
	11	12	13	14	15	16	17	18	19	20
	14	**8**	**4**	**15**	**14**	**20**	**15**	**32**	**40**	**75**

Fig. 4 illustrates the TIM values as the number of data collection networks is altered. Again, the impact of the attack becomes more intense as the IoT network depends on more collection edges. TIM takes values from 0.21 (0.27) to 0.43 (0.52) with respect to the light (heavy) attack mode. In the worst case, where TIM = 0.43 (TIM = 0.43), at least half of the expected data streams are lost due to security attacks in the collection domains, which could be catastrophic for the application that expects those data streams for preparing an output service to the final users. Also, it is quite interesting that the progress of TIM parameter is almost linear, meaning that a potential threat may become more powerful in large-scale IoT systems with many unprotected collection networks.

The accuracy of the introduced analysis is justified by the numerical values of Table IV. This table summarizes the absolute difference between the analytic and the simulated values. The values are expressed in the form of 10^{-4}. In general, the observed error is getting larger as the IoT system becomes larger, i.e., when having more data collection networks. However, that error is marginal, since the maximum recorded difference reaches $75 \cdot 10^{-4}$, having in mind that the modeled IoT system consists of 22 independent nodes.

D. Forwarding Rate Impact

The impact of the forwarding rate in the data collection networks is assessed in this section. The number of the data collection networks is 10. $\mu_i, \forall 1 \leq i \leq N$ varied from 1.5 to 2.5 with a step of 0.5. The arrival rate in each data collection network is identical and equal to 1 data stream per time unit. The arrival rate of the security attacks is 0.5 data

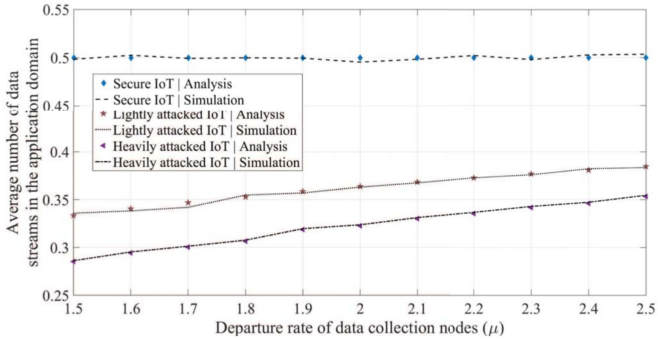

Fig. 5. Average number of data streams in the application domain as the number of the departure rate of the data collection networks is changed.

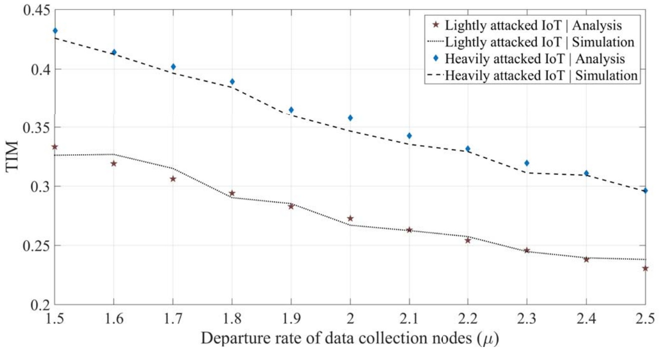

Fig. 6. TIM values as the number of the departure rate of the data collection networks is changed.

streams per time unit. As a result, the data collection networks utilization is in the range of $q_i = (1/0.5 + 1.5) = 0.5$ to $q_i = (1/0.5 + 2.5) = 0.33$. Thus, the stability of the IoT system is ensured. Furthermore, the gateway delivery rate is set equal to 20 data streams per time unit, while the application consuming (departure) rate is set equal to 30 data streams per time unit.

Fig. 5 illustrates the average number of data streams in the application domain as the forwarding rate of each data collection network is varied from 1.5 to 2.5. Accordingly, Fig. 6 depicts the TIM values subject to the forwarding rate change and Table V outlines the analysis error. Two main findings may be pointed out from the obtained curves and numerical results. First, as the departure rate (or forwarding rate) in data collection networks increases the impact of both attack modes disseminates. This phenomenon is attributed to the fact that a high-throughput data collection network forwards more data streams per unit time, hence the probability of losing a data stream due to an attack is smaller. In other words, high-capacity collection networks may contribute to the alleviation of many attack results since they can provide a safer domain in which the collection of the valuable information could be more efficient. For example, TIM in light attack mode begins from about 0.33 and ends at 0.23 given that the forwarding rate was just increased by a unity from 1.5 to 2.5. Second, Table V demonstrates the accuracy of the proposed model. The maximum error reaches $49 \cdot 10^{-4}$, while the average error is about $15 \cdot 10^{-4}$. Moreover, analytic and simulated numerical values are almost identical for all the number of rates (Figs. 5 and 6), a fact that indicates the accuracy of the presented analytic framework.

TABLE V
DIFFERENCE ERROR BETWEEN THE ANALYSIS AND SIMULATION AS THE FORWARDING RATE IS CHANGED

$\cdot \mathbf{10^{-4}}$	**absolute difference** vs forwarding rate (1.5-2.5)					
Secure IoT	1.5	1.6	1.7	1.8	1.9	2
	16	**26**	**7**	**0**	**5**	**45**
	2.1	2.2	2.3	2.4	2.5	
	16	**22**	**20**	**28**	**35**	
Lightly attacked IoT	1.5	1.6	1.7	1.8	1.9	2
	25	**22**	**49**	**19**	**15**	**5**
	2.1	2.2	2.3	2.4	2.5	
	8	**0**	**10**	**14**	**10**	
Heavily attacked IoT	1.5	1.6	1.7	1.8	1.9	2
	12	**9**	**4**	**11**	**24**	**12**
	2.1	2.2	2.3	2.4	2.5	
	22	**25**	**10**	**17**	**11**	

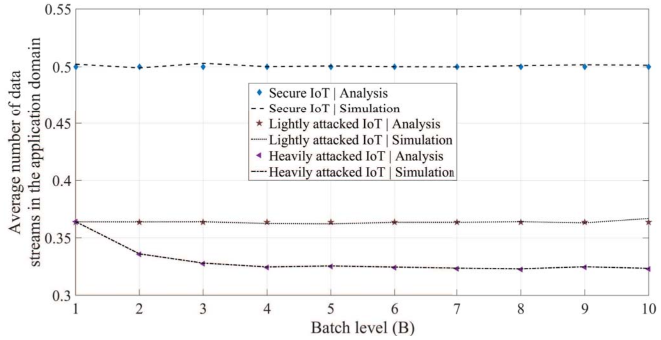

Fig. 7. Average number of data streams in the application domain as the number of the batch level is changed.

E. Batch Level Impact

This section is devoted to the study of the batch level impact. In the following figures, the batch level is varied from 1 (equal to a light attack) to 10. Once more, the arrival rate in each data collection network is identical and equal to 1 data stream per time unit. The arrival rate of the security attacks is 0.5 data streams per time unit. The forwarding rate in each data collection network is 2 data streams per time unit. Also, the gateway delivery rate is set equal to 20 data streams per time unit, while the application consuming (departure) rate is set equal to 30 data streams per time unit. As previously, the stability of the IoT system is ensured.

Fig. 7 illustrates the average number of data streams in the application domain as the number of batch level is changed. As expected, the heavily attacked IoT curve is altered only, while the two others remain stable. The average number of data streams in the application domain is about 0.5. The light attack induces almost 28% losses. The remaining data streams are stable as the batch level is changed. On the contrary, the heavily attacked IoT curve presents an interesting progress. Initially, it is identical with that of the light attack when $B = 1$. Then, it is getting more pressing, i.e., it reduces the average number of data streams by 0.2 and 0.3 when $B = 2$ and $B = 3$, respectively. In addition, when $B = 4$ the impact of the heavy attack is stabilized. This is due to the fact that values larger that $B = 5$ cause no more losses in the data collection

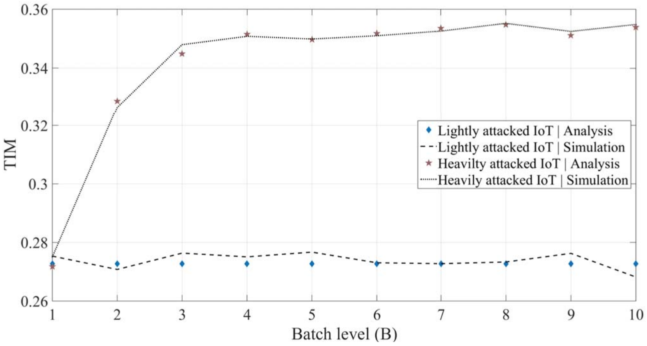

Fig. 8. TIM values as the number of the batch level is changed.

TABLE VI
DIFFERENCE ERROR BETWEEN THE ANALYSIS AND SIMULATION AS THE BATCH LEVEL IS CHANGED

$\cdot\mathbf{10^{-4}}$	**absolute difference** vs batch level (1-10)									
Secure IoT	1 **24**	2 **9**	3 **31**	4 **2**	5 **9**	6 **2**	7 **0**	8 **11**	9 **18**	10 **15**
Lightly attacked IoT	1 **4**	2 **3**	3 **5**	4 **10**	5 **14**	6 **0**	7 **0**	8 **5**	9 **5**	10 **33**
Heavily attacked IoT	1 **5**	2 **12**	3 **9**	4 **12**	5 **20**	6 **6**	7 **4**	8 **19**	9 **33**	10 **40**

networks since the average number of data streams in the data collection nodes is unlikely to be more than $B = 5$. Thus, given the arrival rates and the forwarding rates in the data collection nodes, the heavy attack impact is maximized when $B = 5$.

Fig. 8 verifies the aforementioned remarks. It presents a stable TIM for the light attack and an increased TIM for the heavy attack that reaches its maximum value when $B = 5$ and then remains stable. This point signals the upper bound a distributed attack may have. It points out the maximum negative impact given specific values of arrival and departure rates.

Once again, Table VI indicates the accuracy of the presented analysis, even though the heavy attack scenario is assessed only. The observed error is maximized when $B = 10$, reaching an absolute difference of $40 \cdot 10^{-4}$.

F. Gateway Delivery Rate Impact

Even though the gateway node is not directly affected by either the light or the heavy attack, it is important to investigate how the impact of the external threat is influenced by the gateway delivery rate. In the following figures the gateway delivery rare (or the gateway node departure rate) is varied from 20 to 200 data streams per time unit. At the same time, the consuming rate (or the departure rate) of the application domain is adjusted to this change with respect to a fixed ratio, which is kept 2 : 3 in order to avoid violating the IoT system balance. The other parameters remain unchanged; the data collection arrival rate is equal to 1 data stream per time unit for all collection nodes, the arrival rate of the security attacks is 0.5 data streams per time unit, the forwarding rate in each data collection network is 2 data streams per time unit, and the batch level is fixed and equal to 5 data streams per attack (or negative arrival).

Fig. 9 shows how the average number of data streams are affected by the change in the gateway delivery rate. It should be stressed that the average number of data streams is getting lower as the rate becomes larger. This is attributed to the fact that the gateway forwards faster the data streams to the application domain. In the same way, the application domain consumes faster the incoming data streams from the gateway node. Eventually, as the data streams that remain in the application domain become lower, the affected data streams due to the security attack become less.

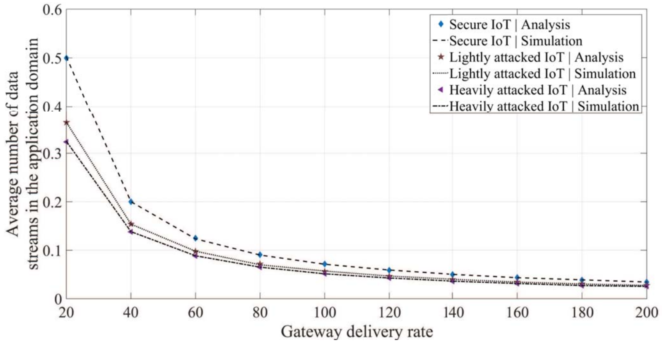

Fig. 9. Average number of data streams in the application domain as the gateway delivery rate is changed.

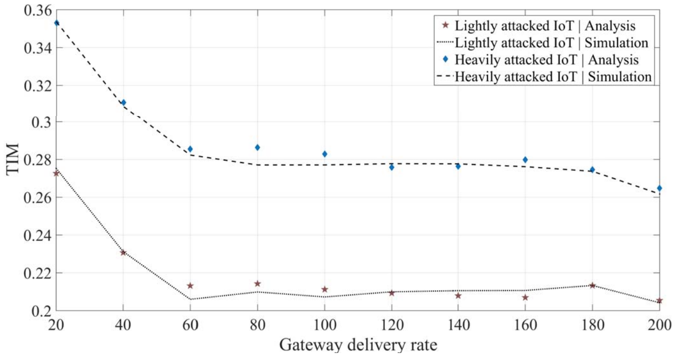

Fig. 10. TIM values as the gateway delivery is changed.

TABLE VII
DIFFERENCE ERROR BETWEEN THE ANALYSIS AND SIMULATION AS THE GATEWAY DELIVERY RATE IS CHANGED

$\cdot\mathbf{10^{-4}}$	**absolute difference** vs gateway delivery rate (1-10)									
Secure IoT	1 **24**	2 **2**	3 **5**	4 **8**	5 **3**	6 **4**	7 **3**	8 **0**	9 **0**	10 **0**
Lightly attacked IoT	1 **4**	2 **0**	3 **1**	4 **7**	5 **4**	6 **0**	7 **2**	8 **1**	9 **8**	10 **1**
Heavily attacked IoT	1 **0**	2 **1**	3 **2**	4 **4**	5 **2**	6 **3**	7 **2**	8 **9**	9 **12**	10 **14**

Fig. 10 sheds light on the security impact as the gateway throughput is changed. Given that the average number of data streams depends on the gateway delivery rate, as (28) dictates, the threat impact is changed subject to the gateway rate change. Initially, the impact is reduced until $\mu_{N+1} = 60$. Then it remains almost stable and finally, it slightly drops again ($\mu_{N+1} = 200$). This phenomenon indicates that high-throughput gateway nodes might positively, yet slightly, affect the absorption of external attacks.

Table VII summarizes the analysis error for all ten values of the gateway delivery rate. At this case, the error is quite limited since the rate of both positive and negative arrivals in the

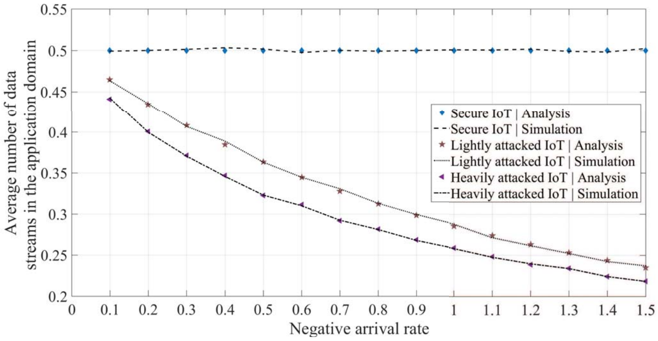

Fig. 11. Average number of data streams in the application domain as the negative arrival rate is changed.

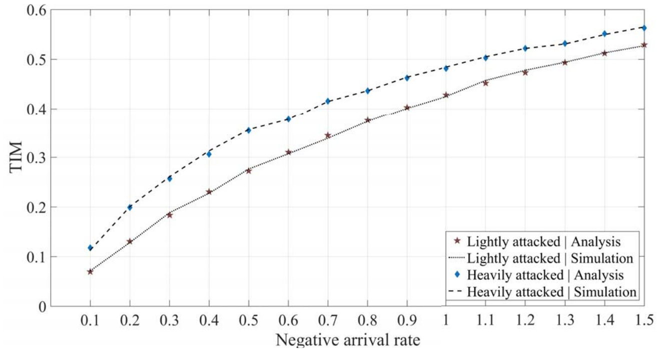

Fig. 12. TIM values as the negative arrival rate is changed.

data collection networks remains fixed and only the gateway delivery rate is changed. Hence, the error rate depends only on one node (gateway) rather than N nodes as in the previous cases.

G. Attack Rate Impact

Finally, in this section, the rate of the attack is examined. The negative arrival rate is changed from 0.1 to 1.5 data streams per time unit. The data arrival remains 1 data stream per time unit and the departure rate is fixed at 2 data streams per time unit for all the data collection networks. The delivery rate of the gateway is 20 data streams per time unit and the consuming rate of the application domain is fixed and equal to 30. The batch level is fixed and equal to 5 data streams per attack (or negative arrival). In essence, this section investigates the case, where the arrival rate of the security attacks becomes larger than that of the data streams.

Fig. 11 depicts the average number of data streams as a function of the change in the attack rate. As expected, both attack modes become more intense as the negative arrival rate is increased. Given an average number of data streams equal to 0.5, the light attack reduces this number up to 0.24 when the negative arrival rate is maximized. In the same way, the heavy attack applies even more impact to the IoT system by reducing this number up to 0.22. Thus, almost half of the expected incoming traffic is lost when the negative arrival rate becomes 50% larger than the traffic arrival rate. Fig. 12 verifies this statement. The impact of both attack modes becomes even stronger following an almost linear increase. Finally, Table VIII summarizes the error analysis, which is quite limited. The maximum absolute difference between the analysis and the simulation appears when the negative arrival rate is 0.4 in the case of the secure IoT, and it is equal to $34 \cdot 10^{-4}$

TABLE VIII
DIFFERENCE ERROR BETWEEN THE ANALYSIS AND SIMULATION AS THE ATTACK ARRIVAL RATE IS CHANGED

$\cdot 10^{-4}$	**absolute difference** vs attack rate change (0.1-1.5)							
Secure	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8
IoT	**7**	**2**	**15**	**34**	**18**	**23**	**3**	**7**
	0.9	1	1.1	1.2	1.3	1.4	1.5	
	2	**9**	**7**	**17**	**10**	**17**	**24**	
Lightly	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8
attacked	**15**	**11**	**12**	**41**	**5**	**0**	**29**	**6**
IoT	0.9	1	1.1	1.2	1.3	1.4	1.5	
	10	**21**	**24**	**13**	**8**	**13**	**21**	
Heavily	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8
attacked	**2**	**5**	**7**	**11**	**4**	**12**	**9**	**3**
IoT	0.9	1	1.1	1.2	1.3	1.4	1.5	
	12	**5**	**3**	**11**	**16**	**22**	**24**	

VI. CONCLUSION

A novel analytic model for formulating an IoT system under attack is presented in this paper. The G-network concept is adopted since it is suitable for modeling security attacks by considering negative arrivals. The proposed model is presented in detail and key performance metrics are introduced. The accuracy of the provided closed-formed equations is extensively assessed in a realistic simulation environment. Simulation results verify the robustness of our model, while considerable performance behaviors are highlighted. Our future plans include the expansion of the G-network model in analyzing more forms of attack in upper layers. For instance, we intend to analyze the impact of routing attacks in the network layer by using a more complex analytic model compared to the one presented in this paper. In addition, our future endeavors will focus on combining modern threat detection systems with analytic models. For example, we design a visual-based security threat detection scheme for IoT applications which will be able to directly exploit the research outcomes of this paper to effectively expose various external attacks in multiple IoT layers.

REFERENCES

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, “Internet of Things for smart cities,” *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[2] S. Chatterjee and S. Misra, “QoS estimation and selection of CSP in oligopoly environment for Internet of Things,” in *Proc. IEEE Wireless Commun. Netw. Conf.*, Doha, Qatar, Apr. 2016, pp. 1–6.

[3] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, “A software defined networking architecture for the Internet-of-Things,” in *Proc. IEEE Netw. Oper. Manag. Symp. (NOMS)*, Kraków, Poland, May 2014, pp. 1–9.

[4] A. Ghanbari, Ó. Álvarez, and J. Markendahl, “Internet of Things: Redefinition of business models for the next generation of telecom services,” in *Proc. 26th Eur. Regional Conf. Int. Telecommun. Soc. Madrid (ITS)*, 2015. [Online]. Available: https://www.econstor.eu/handle/10419/127142

[5] E. Gelenbe and C. Morfopoulou, *Routing and G-Networks to Optimise Energy and Quality of Service in Packet Networks* (Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering), vol. 54. Heidelberg, Germany: Springer, 2011, pp. 163–173. [Online]. Available: https://link.springer.com/book/10.1007/978-3-642-19322-4#page=168

[6] B. Xiong, K. Yang, J. Zhao, W. Li, and K. Li, "Performance evaluation of OpenFlow-based software-defined networks based on queueing model," *Comput. Netw.*, vol. 102, pp. 172–185, Jun. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S138912861630069X

[7] J. M. Fourneau and K. Wolter, *Some Applications of Multiple Classes G-Networks With Restart* (Communications in Computer and Information Science), vol. 659. Cham, Switzerland: Springer, 2016, pp. 126–133. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-47217-1_14

[8] E. Gelenbe, "G-networks with signals and batch removal," *Prob. Eng. Inf. Sci.*, vol. 7, no. 3, pp. 335–342, 1993. [Online]. Available: https://www.cambridge.org/core/article/div-class-title-g-networks-with-signals-and-batch-removal-div/5E6E9172810894893FB71F5265B45379

[9] P. P. Bocharov and V. M. Vishnevskii, "G-networks: Development of the theory of multiplicative networks," *Autom. Remote Control*, vol. 64, no. 5, pp. 714–739, 2003.

[10] R. H. Weber, "Internet of Things—New security and privacy challenges," *Comput. Law Security Rev.*, vol. 26, no. 1, pp. 23–30, 2010.

[11] F. Mattern and C. Floerkemeier, "From the Internet of computers to the Internet of Things," in *From Active Data Management to Event-Based Systems and More* (Lecture Notes in Computer Science), vol. 6462. Heidelberg, Germany: Springer, 2010, pp. 242–259. [Online]. Available: https://link.springer.com/book/ 10.1007/978-3-642-17226-7#page=255

[12] M. Medwed, "IoT security challenges and ways forward," in *Proc. ACM 6th Int. Workshop Trustworthy Embedded Devices (TrustED)*, Vienna, Austria, 2016, p. 55. [Online]. Available: http://doi.acm.org/10.1145/2995289.2995298

[13] E. Bertino, K.-K. R. Choo, D. Georgakopolous, and S. Nepal, "Internet of Things (IoT): Smart and secure service delivery," *ACM Trans. Internet Technol.*, vol. 16, no. 4, pp. 1–7, Dec. 2016. [Online]. Available: http://doi.acm.org/10.1145/3013520

[14] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Netw.*, vol. 20, no. 8, pp. 2481–2501, 2014.

[15] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the Internet of Things," *Computer*, vol. 46, no. 4, pp. 46–53, 2013.

[16] W. Zhang and B. Qu, "Security architecture of the Internet of Things oriented to perceptual layer," *Int. J. Comput. Consum. Control*, vol. 2, no. 2, pp. 37–45, 2013.

[17] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, and A. Iera, "A systemic and cognitive approach for IoT security," in *Proc. Int. Conf. Comput. Netw. Commun. (ICNC)*, Honolulu, HI, USA, 2014, pp. 183–188.

[18] A. Ukil, J. Sen, and S. Koilakonda, "Embedded security for Internet of Things," in *Proc. 2nd Nat. Conf. Emerg. Trends Appl. Comput. Sci. (NCETACS)*, Shillong, India, 2011, pp. 1–6.

[19] E. Welbourne *et al.*, "Building the Internet of Things using RFID: The RFID ecosystem experience," *IEEE Internet Comput.*, vol. 13, no. 3, pp. 48–55, May/Jun. 2009.

[20] J. Lin *et al.*, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, to be published.

[21] X. Yang *et al.*, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, Jan. 2015.

[22] Q. Yang *et al.*, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[23] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Proc. IEEE/ACM 3rd Int. Conf. Cyber Phys. Syst. (ICCPS)*, Beijing, China, 2012, pp. 183–192. [Online]. Available: http://dx.doi.org/10.1109/ICCPS.2012.26

[24] D. Seal, *ARM Architecture Reference Manual*. London, U.K.: Pearson Educ., 2001.

[25] E. Gelenbe, "Product-form queueing networks with negative and positive customers," *J. Appl. Prob.*, vol. 28, no. 3, pp. 656–663, 1991. [Online]. Available: http://www.jstor.org/stable/3214499

[26] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of Internet of Things (IoT)," *Int. J. Comput. Appl.*, vol. 111, no. 7, pp. 1–6, 2015.

[27] E. Gelenbe, G. Pujolle, and J. Nelson, *Introduction to Queueing Networks*. Chichester, U.K.: Wiley, 1998.

[28] S. Misra, P. V. Krishna, K. I. Abraham, N. Sasikumar, and S. Fredun, "An adaptive learning routing protocol for the prevention of distributed denial of service attacks in wireless mesh networks," *Comput. Math. Appl.*, vol. 60, no. 2, pp. 294–306, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0898122110000088

[29] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Comput. Netw.*, vol. 57, no. 10, pp. 2266–2279, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613000054

[30] J. R. Douceur, *The Sybil Attack* (Lecture Notes in Computer Science), vol. 2429. Heidelberg, Germany: Springer, 2002, pp. 251–260. [Online]. Available: https://link.springer.com/chapter/10.1007%2F3-540-45748-8_24?LI=true

[31] N. Kumar, S. Misra, J. J. P. C. Rodrigues, and M. S. Obaidat, "Coalition games for spatio-temporal big data in Internet of Vehicles environment: A comparative analysis," *IEEE Internet Things J.*, vol. 2, no. 4, pp. 310–320, Aug. 2015.

[32] J. Lin *et al.*, "A novel dynamic en-route decision real-time route guidance scheme in intelligent transportation systems," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst.*, Jun. 2015, pp. 61–72.

[33] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops)*, Mar. 2017, pp. 618–623.

[34] L. Belli *et al.*, "Design and deployment of an IoT application-oriented testbed," *Computer*, vol. 48, no. 9, pp. 32–40, Sep. 2015.

Panagiotis Sarigiannidis (S'06–A'07–M'13) received the B.Sc. and Ph.D. degrees in computer science from the Aristotle University of Thessaloniki, Thessaloniki, Greece, in 2001 and 2007, respectively.

He is currently an Assistant Professor with the University of Western Macedonia, Kozani, Greece. He has authored or co-authored over 90 papers in international journals, conferences, and book chapters. He has been involved in several national and international research projects. His current research interests include optical and wireless network modeling, resource allocation, optimization, intrusion detection, and networking protocols.

Eirini Karapistoli (S'03–A'08–M'12) received the Ph.D. degree in electrical engineering from the Aristotle University of Thessaloniki, Greece, in 2009 and the M.B.A. degree in project management from the Blekinge Institute of Technology, Karlskrona, Sweden, in 2013.

She is the Technical Director (CTO) with CapriTech Limited, Essex, U.K. She has co-authored over 30 peer-reviewed publications in scientific journals and international conferences. She is involved in a range of activities including software architecting and development, research and development proposals preparation, and project executions. She has a broad expertise in game theory applied to communication networks, as well as in network intrusion detection, and mathematical optimization.

Dr. Karapistoli was a recipient of the Post-Doctoral Research Grant from 2012 to 2015 from the Greek Secretariat of Research and Technology.

Anastasios A. Economides (S'83–M'92–SM'09) received the Ph.D. degree in computer engineering from the University of Southern California, Los Angeles, CA, USA.

He is a Full Professor of computer networks and telematic applications (CONTA) with the University of Macedonia, Thessaloniki, Greece, where he is the Deputy Representative of EL.ID.E.K. (the official administration for the National/Greek Research Policy). He is the Director of the CONTA Laboratory, University of Macedonia, where he was the Chairman of the Information Systems Postgraduate Program from 2008 to 2014. He has been a Visiting Professor with several universities such as the University of Southern California, Los Angeles, Universitat Oberta de Catalunya, Barcelona, Spain, and Universitat Pompeu Fabra, Barcelona. He has authored or co-authored over 200 peer-reviewed papers and has received over 3000 citations. His current research interests include Internet of Things, user experience and acceptance of smart systems and services, networking protocols, and techno-economics and competition.

Dr. Economides has been the Plenary Speaker at international conferences on Internet of Things and on computer-based assessment. He has been the Principal Investigator of many funded projects.