electronics

MDPI

Article

A Framework for Mitigating DDoS and DOS Attacks in IoT Environment Using Hybrid Approach

Abdulrahman Aminu Ghali *, Rohiza Ahmad and Hitham Alhussian

Computer & Information Sciences Department, Universiti Teknologi PETRONAS, Seri Iskandar 32610, Perak Darul Ridzuan, Malaysia; rohiza_ahmad@utp.edu.my (R.A.); seddig.alhussian@utp.edu.my (H.A.)

* Correspondence: aminuabdulrahman81@yahoo.com

Abstract: The Internet of Things (IoT) has gained remarkable acceptance from millions of individuals. This is evident in the extensive use of intelligent devices such as smartphones, smart television, speakers, air conditioning, lighting, and high-speed networks. The general application area of IoT includes industries, hospitals, schools, homes, sports, oil and gas, automobile, and entertainment, to mention a few. However, because of the unbounded connection of IoT devices and the lack of a specific method for overseeing communication, security concerns such as distributed denial of service (DDoS), denial of service (DoS), replay, botnet, social engineering, man-in-the-middle, and brute force attacks have posed enormous challenges in the IoT environment. Regarding these enormous challenges, this study focuses on DDoS and DoS attacks. These two attacks have the most severe consequences in the IoT environment. The solution proposed in this study can also help future researchers tackle the expansion of IoT security threats. Moreover, the study conducts rigorous experiments to assess the efficiency of the proposed approach. In summary, the experimental results show that the proposed hybrid approach mitigates data exfiltration caused by DDoS and DoS attacks by 95.4%, with average network lifetime, energy consumption, and throughput improvements of 15%, 25%, and 60%, respectively.

Keywords: IoT; DDoS; DoS; security challenges; LEACH

Citation: Ghali, A.A.; Ahmad, R.; Alhussian, H. A Framework for Mitigating DDoS and DoS Attack in IoT Environment Using Hybrid Approach. *Electronics* **2021**, *10*, 1282. https://doi.org/10.3390/electronics10111282

Academic Editor: Sang-Soo Yeo and Damien Sauveron

Received: 24 April 2021
Accepted: 24 May 2021
Published: 27 May 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Internet of Things (IoT) has proven to be a new trend for government, education, sports, industries, military, and oil and gas. It is projected that the acceptance of IoT will keep growing. Nowadays, there are over 23 billion IoT-connected devices worldwide. This number will continue to rise until it reaches 30 billion by the year 2025, and perhaps over 60 billion by the end of 2030 [1,2].

The fundamental idea of IoT is linking up smart devices to communicate through the internet. These smart devices are equipped with sensors connected to the internet that are uniquely identifiable, communicating with each other to perform complex tasks [3,4]. As such, these devices require the ability to collect, process, and transmit data through various channels [5].

The advent of the IoT has provided industries like oil and gas, transportation, healthcare, education, homes, sports, and automobile industries with new and innovative ways of handling business operations, including procurement, manufacturing, and the distribution of goods and services [6,7]. The advantage of the IoT is that it enables devices (things) to send and receive data from one another when connected, and to control the operations of other devices remotely [8]. For instance, IoT can be employed for a smooth gas pipeline operation, where a temperature sensor attached to the gas pipeline can aid the endeavor. The sensor emits readings to an engineer's mobile phone, who can then remotely

shut off the pipeline in case of a data abnormality. This occurs because of the unbounded connections of IoT devices, which communicate with one another. On the other hand, because of the possibility of the connections and no single owner/party overseeing the communications, security issues such as DDoS and DoS attacks become a significant challenge in the IoT environment [9,10]. Figure 1 illustrates the basics of IoT technology.

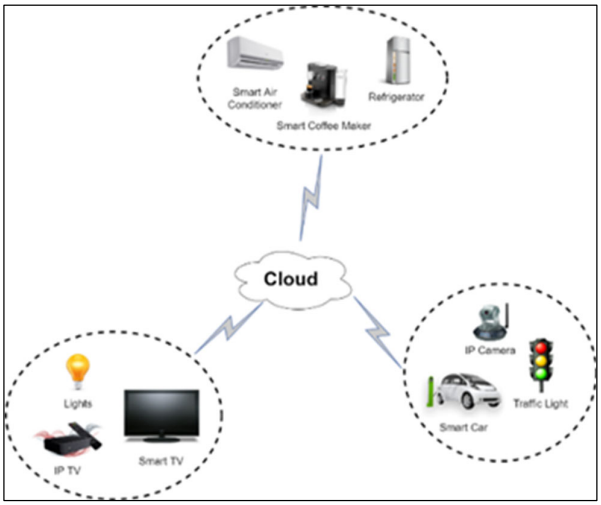


Figure 1. The basics of Internet of Things (IoT) technology.

With the increasing interconnectivity of IoT devices and the lack of an entity preventing communications in IoT, security challenges such as DDoS and DoS attack become a critical challenge, and they have attracted the attention of stakeholders in the IoT environment to provide substantial solutions [11–14]. Although these challenges occur in other environments, their impact can be more harmful in the IoT environment, which is worrisome as it enables intruders to penetrate the environment. These attacks have several consequences that may lead to financial loss in IoT as well as in other various organizations.

Furthermore, existing literature studies have not focused on data exfiltration caused by DDoS and DoS attacks. There is an inadequate clear explanation of the existing methodology of the problem mentioned above. In contrast, the existing literature focuses on the general idea of DDoS and DoS attacks. For this reason, the study also adopts a low-energy adaptive clustering hierarchy (LEACH) to enhance IoT's network lifetime, energy consumption, and throughput to mitigate the DDoS and DoS attacks in the IoT environment. Safeguarding the data and nodes is a consideration of paramount importance for securing communication.

Data exfiltration is a type of security breach in an IoT environment as a result of DDoS and DoS attacks in which data are copied and transferred without the owner's consent [15]. As such, this study brings a holistic and robust method to address these problems. This study set a fresh random key so as to ensure the nodes were validated. The fresh random keys also assisted in ensuring no nodes communicated with the cluster head (CH) without authentic validation. The consideration of the four parameters, namely, security, network lifetime, energy consumption, and throughput, produced a robust approach as a hybrid.

In recent years, several researchers have studied the security challenges in the IoT environment. These challenges include replay, botnet, social engineering, man-in-the-middle, and brute force attacks, which have led to significant financial losses [16–18]. None of these works provided an in-depth study on the exfiltration attack caused by DDoS and DoS attacks in the IoT environment.

Rigorous experiments are conducted throughout this study to assess the efficiency of the proposed approach. The experimental results show that the proposed hybrid

approach mitigates the data exfiltration of DDoS and DoS attacks with about 95.4% improvements, and with average improvements in the network lifetime, energy consumption, and throughput of 15%, 25%, and 60% respectively.

The remainder of this study is as follows: Section 2 discusses the motivation and related work. Section 3 describes the methodology. Section 4 provides the results. Finally, Section 5 concludes the study.

2. Motivation and Related Work

In recent years, many review papers have been published on IoT, with the aim of research purpose and scientific knowledge [19]. However, most of these studies focused on general issues instead of specific issues as highlighted in this study. The following section will highlight the related work of the existing studies.

In the study in [20], the authors presented various research findings based on IoT security threats and challenges. According to the findings, authentication and integrity should be given utmost priority in order to withstand proxy and man-in-the-middle attacks. On the other hand, this study did not consider specific issues regarding DoS and DDoS attacks in the IoT environment.

In [20], the researchers described the importance of the security requirements in the IoT environment, and the study further divided the security requirement into various categories. These were confidentiality, authentication, and access control, while the dangers of DDoS and DoS attacks were not considered.

In [21], the security concern was detailed only from a privacy point of view, while other applicable security issues were left unattended. In the work of [22], the authors proposed various architectures of IoT layers and their challenges. Among these layers, problems were identified that were related to communication, namely, quality of service (QoS), the vast number of objects, transport control protocol, and real-time object detections, among others. Thus, the threat of DoS and DDoS attacks remains unidentified.

In the study in [23], the researchers identified architectural layer issues in the IoT environment. The layers included (i) the perception layer. Among this layer's problems is unauthorized access to the tags, tag cloning, eavesdropping, spoofing, and Radio Frequency (RF) jamming. (ii) The network layer problems included Sybil attack, sinkhole attack, sleep deprivation attack, malicious code injection, and man-in-the-middle attack. Lastly, (iii) the application layer. The challenges that constituted this layer included malicious code injection, spear-phishing attack, DoS attack, and sniffing attack.

The work in [24] identified IoT security challenges as worrisome to the IoT environment. Based on their findings, the authors divided the security challenges into three aspects. These were the M2M layer, with the attacks such as jamming, deactivation, tampering, collision, and exhaustion. The second problem identified was the network layer attack, which included hello flood, sinkhole, Sybil attack, selective forwarding/gray, eavesdropping, and traffic analysis problems. The last issue was the cloud layer attacks, which comprised flooding, malware, spoofing, message forging, and intersection.

In the study by [25], the authors divided IoT challenges into internal and external attacks. Internal attacks have more severe consequences than external attacks. In internal attacks, the attacker gains access to the network by compromising the IoT nodes, and further disguises them as genuine node. The attack leads to various threats to the IoT environment. On the other hand, the external attacks create traffic congestion and fake routing updates to the network. The attacks cause anomalous functionalities to the network, in which active and passive attacks are initiated. Hence, there are no specific detailed solutions on how DDoS and DoS attacks can be tackled.

In [26], they described IoT challenges as one of the factors presenting obstacles to the IoT environment. Based on the investigation, it was revealed that telnet-based attacks were one of the critical attacks, and they have escalated since 2014. The attack compromises IoT devices by not allowing devices to connect. Such attacks promote the misuse of user data.

In the review of [27], the authors discovered that confidentiality, access control, integrity, and authentication were of the utmost security concern for the IoT. The study also pointed out that the user data are critical to consider as one of the aspects that need to be protected in the IoT environment. Hence, if data confidentiality, integrity, and authentication are given the utmost priority in the IoT environment, it will resolve many vulnerability issues.

The research in [28] divided IoT security challenges into three main categories. These are data confidentiality, privacy, and trust. Confidentiality represents the IoT environment's fundamental issues where security is not guaranteed to legitimate users in order to access their data. Privacy is another fundamental issue in the IoT environment. For instance, the health care system represents one of the most significant applications in the IoT environment. The comparison of the proposed approach based on the existing algorithms is shown in Table 1.

Table 1. Comparison of the proposed approach with the existing algorithms.

	Existing Algorithms					Proposed Hybrid Approach		
Attacks	**Authors**	**Algorithm**	**Design Components**	**Secuirty Objectives**	**Technology**	**Energy Consumption**	**Lifetime**	**Throughput**
DDoS or DoS	[29]	SDN	IoT	Secure communication	RFID Smart city	-	1600	2400
	[30]	Ms-LEACH	-	Secure communication	WSN	1	42	7.6
	[31]	I-LEACH	IoT	-	WSN	-	1750	-
	Existing LEACH approach	LEACH	IoT	Secure communication	RFID	162.71	236	193,806
	Proposed approach	Hybrid approach	IoT	Secure communication	RFID	152.58	275	253,297

Based on the table above, the research study compared the existing algorithms with the proposed approach. The comparison was based on the following parameters, namely security, energy consumption, lifetime, and throughput. It is believed that a comparison of the parameters can add more significance to the study findings. Among the impact of the study, security enhancement, network lifetime, energy reservation of the nodes, and measuring the data transferred in a specific time as throughput added value to the study. Thus, the proposed hybrid approach will provide a research gap for future researchers. As observed in Table 1, we compared the parameters of algorithms such as MS-LEACH based on percentages. While for other algorithms, such as I-LEACH, we did not provide in-depth details about energy consumption and throughput. In addition, we did not provide the energy consumption results for the SDN algorithm. This shows that the proposed hybrid approach underwent rigorous experiments to improve security, and further enhanced parameters such as lifetime, energy consumption, and throughput. It can be seen that the proposed hybrid approach consumes less energy compared with the existing algorithms. The factors of lifetime and throughput showed encouraging results compared with the other algorithms.

3. Methodology

In this section, the execution method of the hybrid method is displayed. This study enhanced low-energy adaptive clustering hierarchy (LEACH) to improve the security and IoT network lifetime, energy consumption, and throughput in order to mitigate DDoS and DoS attacks in the IoT setting. To secure communication, it is critical to understand data, and node security is crucial. Therefore, the research focused more on securing data against DDoS and Dos attacks rather than cluster head selection. The diagram of the proposed approach is depicted in Figure 2.

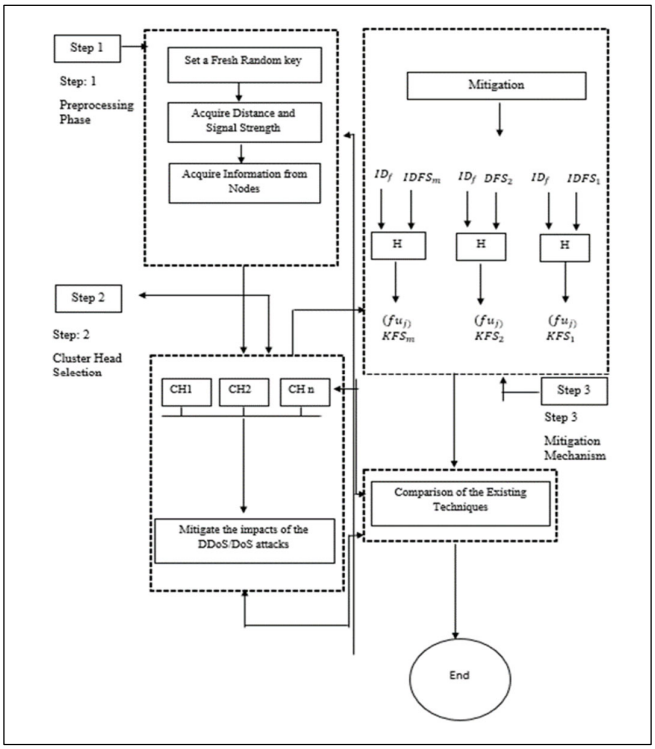


Figure 2. Proposed hybrid approach.

Based on Figure 2, the proposed approach was divided into three steps. Step one is the preprocessing phase. Step two is the cluster head selection phase. Step three is the mitigation mechanism phase. The figure aims to guide the study in order to achieve its intended aims of mitigating DDoS and DoS attacks. Each step performs a significant role in withstanding attacks. In step one, random keys are formed; in step two, cluster heads are developed; and in step three, their energy transmission during the mitigation of attacks is achieved. More details of the steps are explained in Sections 3.1–3.3, respectively.

3.1. Preprocessing Phase

In this approach, the study began by setting a fresh random key to mitigate attacks by intruders, especially DDoS and DoS attacks, which have been identified as the most unsafe attacks in the IoT environment. The keys were set based on the fresh random keys from various nodes. The election of keys was the same as for the cluster heads, based on the wireless sensor network (WSN). The election of the key solely depended on the distance and signal of the nodes. Once the key is set, the information will be acquired from the nodes. The fresh random keys assisted the method in discarding many requests that were not validated from the nodes. However, the random key always decided when the malicious node was not successful in decrypting the authorization keys of the normal sensor nodes. In addition, the random key aimed to secure the communication within the nodes, so that no single node could communicate with its neighbor nodes and CH without validation. This aids in intercepting various unknown requests from DDoS and DoS attacks.

3.2. Cluster Head Selection

The LEACH algorithm operates on several rounds, where each round comprises two phases: the setup and steady phases [31].

In the setup phase, clusters were formed, and the cluster head (CH) was selected. Each node in the cluster could potentially be selected as the CH through a process of

generating a random priority value between 0 and 1. For instance, if the number for the member node is less than the threshold value $T_{(n)}$, then the node will automatically be the CH. Whereas, if the value of the threshold $T_{(n)}$ is given by Equation (1), then the CH is responsible for assigning the TDMA schedule for the particular corresponding cluster members.

$$T_{(n)} = \begin{cases} \dfrac{1}{1 - p\left(r \bmod \dfrac{1}{p}\right)} & \forall n \in \\ 0 \end{cases} \quad (1)$$

where ρ is the percentage of the sensor nodes that could be the CH, r donates the existing round, and G is the set of nodes that not considered in the CH selection process in the earlier $1/p$ rounds. Meanwhile, the node that is preferred as the CH for the specific round r is not permitted to participate in the next $1/p$ rounds. Thus, every sensor node in the cluster can get an equal chance to be the CH. In contrast, the energy dissipation between the sensor nodes is distributed equally in the IoT network.

In the steady phase, the cluster broadcasts the sensed data to the specific CH based on the TDMA schedule. In this way, any node can broadcast data during a specific allotted time slot while the other nodes have the chance to rest. Using the TDMA method, intra-collision issues are avoided. The LEACH algorithm aims to improve energy efficiency using a rotation-based CH selection process using a random number.

Based on the distance between the sensing and receiving nodes, the ratio model is divided into free-space and multi-path fading models, as explained in [31]. Hence, the communication channel is supposed to be symmetrical, and the energy consumed by the sensor node sends the k bits packet to the node d meters, as stated in [32]. The Equation is described below.

$$E_{Tx}(K, d) = E_{Tx\_elec(K)} + E_{Tx\_amp}(k, d) \quad (2)$$

$$E_{Tx}(K, d) = E_{elec} * k + E_{fs} * k * d^2, d \le d_0 \quad (3)$$

$$E_{elec} * k + E_{amp} * k * d^4, d > d_0 \quad (4)$$

Equally, the energy consumes by the sensor node receiving k bits/packets is shown using Equation (5).

$$E_{Rx}(K) = E_{Rx\_elec}(k) + kE_{elec} \quad (5)$$

where E_{elec} is the energy consumption per bits by the transmitter and the receiver, and E_{amp} and E_{fs} are the amplifier parameters of transmission corresponding for the multi-path padding and free space model, respectively.

3.3. Mitigation Mechanism

The study paper aims to address DDoS or DoS attacks in the IoT environment, which lead to data exfiltration. Addressing these issues will prevent IoT users from financial losses and denial of services. Additionally, the generation of the secret keys for the user and server ($FU - FS$) is adapted from the work in [33]. For instance, the mitigation of the attack between the FU and FS is achieved by determining the $FU - FS$ secret key $K_{FS}^{(FU)} = H(ID_F, ID_{FS}, kFU)$, which is used to encrypt and decrypt the session key $k_s, EK_{FS}^{(FU)}, (r\ FS, ks))$ by FU and $D\ K_{FS}^{(FU)}, EK_{FS}^{(FU)}, (r\ FS, ks))$ by FS. This determines that the session key ks is not common to FU and FS, unless the encryption and decryption are performed using the same secret key $K_{FS}^{(FU)}$. The fog user (FU) generates the secret key $K_{FS}^{(FU)}$ locally, using a master key (k_{FU}) and claims the server identity ID_{FS}. Furthermore, the RA generates $K_{FS}^{(FU)}$ in the same way to deliver it secretly to the server. Thus, when the server identity ID_{FS} is alleged without knowing the $K_{FS}^{(FU)}$, the server will not be verified by a genuine user. Moreover, the fog user that does not hold the correct k_{FU} matching his

identity ID_{FU} as stored on the server, will never be varied by the server. The mitigation of the DoS and DDoS attacks is shown in the example below. Assume the intruder sends a DoS or DDoS attack to deny data to transfer between the FU and FS during the mitigation phase between the nodes and CH. The intruder sends a request with the aim of impersonating the FU or FS. Nonetheless, attempting to send a huge request from the various sessions the encrypted key k_s will not authorize the communication unless the attackers override the mitigation phase, which is not possible. For instance, an intruder sends an attack such as DoS or DDoS to the server. The server FS will immediately respond as (ID_{Fs} , ID_F , ID_{FU} , $E\ K_{FS}^{(FU)}$, $r\ FU$, $r\ FS$) to challenge the FU. The server FS will immediately decrypt using $K_{FS}^{(FU)} \neq k^*$, following in $r^*\ FS \neq r\ FS$, and therefore the $r\ FS$ generated by FS is equal to receive only with minor probability. Therefore, the intruder will not succeed in the third round or after many rounds of trial. The results based on the above steps are fully deterministic.

4. Result and Discussion

The development of the result is based on the three stages depicted in Figure 3. The outcomes of the proposed hybrid approach are shown in Table 1 and Figure 4. The research study employed MATLAB R2021a (9.10.0.1 1602886), Windows 10 with 11 Gen Intel (R) Core i7 processor, 3.40 GHz, and 16 GB RAM to achieve the proposed hybrid approach. The simulation parameters are depicted in Table 2. The following figures will show the results based on the energy consumption, lifetime, and throughput parameters.

Table 2. Simulation Parameters.

No	Description Parameters	No. Item Description Parameter
1	Field size	400 × 400
2	Sink location	(200–400)
3	Number of normal nodes	400
4	Number of cluster head	1
5	Field area	X by Y
6	Initial energy of all normal nodes	0.5
7	Initial energy of malicious nodes	0.5 × 10
8	Transmission energy (ETX), reception energy (ERX)	50 × 0.000000001
9	Efs	10 × 0.000000000001
10	Data aggregation energy (EDA)	5 × 0.000000001

Based on Table 2, the study provided description parameters such as the selected values in order to ensure that the findings produced accurate results. For instance, knowing the field size is of paramount important in order to know how many nodes can be mounted in the field area. In addition, it assists in knowing the number of cluster heads. The sink location performs a vital role in collecting all of the data from the sensor nodes and this data are forwarded to the sink node. Thus, the setting of the sink node has a positive impact on the energy consumption and lifetime. Knowing the total number of the normal nodes also aids in selecting the CHs and energy transmission within the nodes. For the CH, the nodes gather their data and pass it to the CHs, and this data are sent to the BS via the CHs. The field area is to know the actual size of the scale area where the nodes will be placed. The study placed the initial energy of the nodes in order to determine the energy capacity of each node. In addition, the study classified the initial energy of malicious nodes in order to understand the capability of the attacks. The node is responsible for transmission energy (ETX), while the energy is consumed during the reception of energy (ERX). The Efs is the amplifier energy used in transmitting and measuring data between nodes distances, whereas data aggregation energy (EDA) is the energy

dissipated per bit to aggregate the message signal. Most importantly, the selection of the parameters has an impact on the energy efficiency, lifetime, and throughput of the IoT network.

Figure 3 describes the energy consumption based on the simulation parameters.

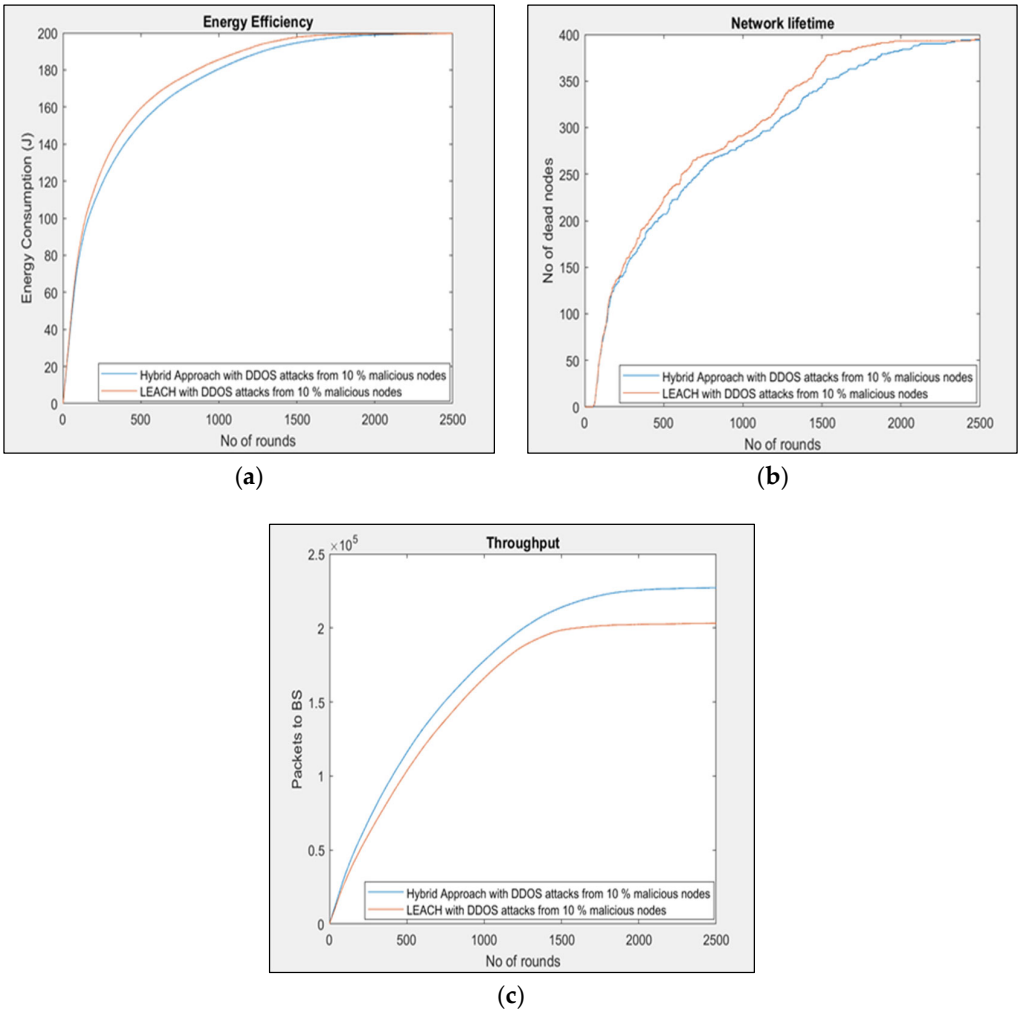


Figure 3. (**a**) Energy consumption with 10% per nodes, (**b**) network lifetime with 10% malicious nodes, and (**c**) throughput with 10% malicious nodes.

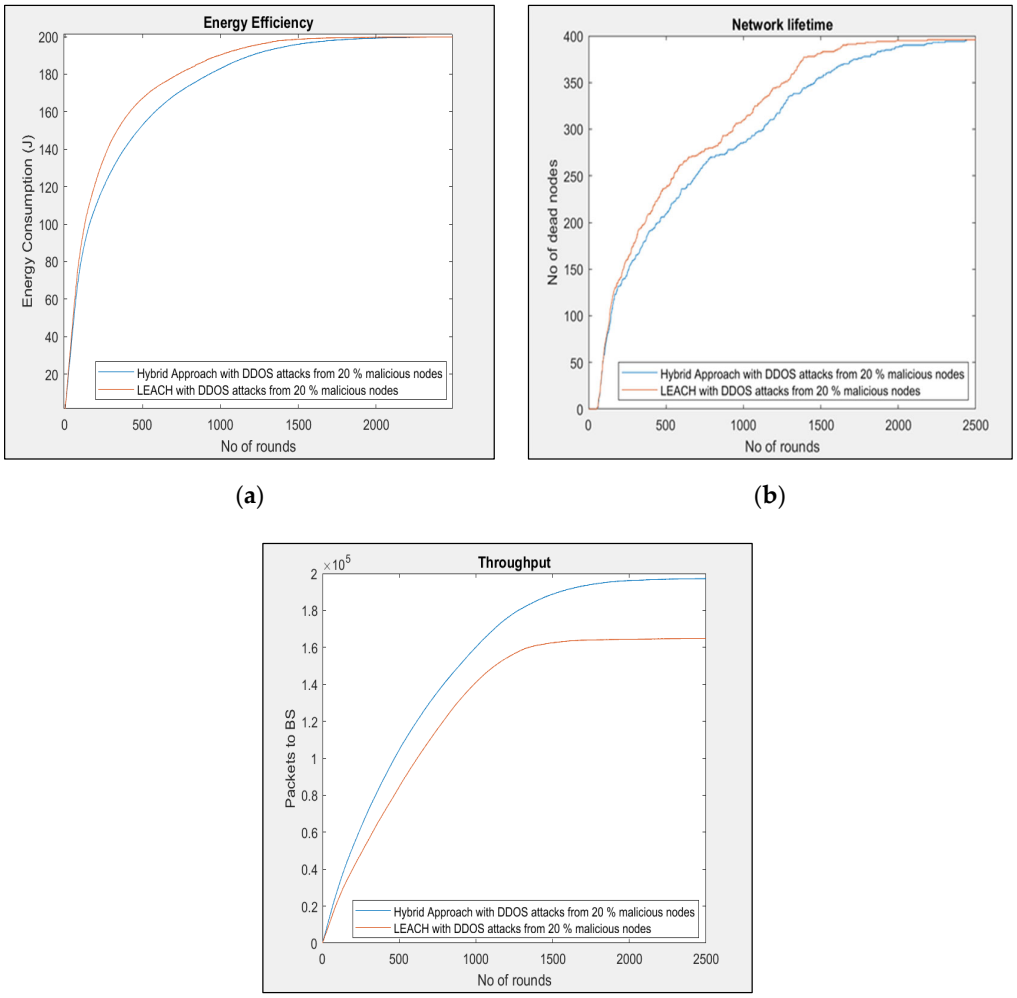


Figure 4. (**a**) Energy consumption with 20% malicious nodes, (**b**) network lifetime with 20% malicious nodes, and (**c**) throughput with 20% malicious nodes.

Based on Figure 3, energy consumption is extremely crucial as part of the protocol for the development of performance evaluation in the IoT network. The Figure indicates that the energy consumption of the existing LEACH with malicious nodes is not encouraging, as depicted in above Figure 3a. Furthermore, the study considered the energy consumption between the malicious nodes, such as DoS and DDoS, and further investigated the proposed hybrid approach. Based on these results, the proposed hybrid approach consumed less energy with 10% malicious nodes with a 0.05 to 0.25 cluster head probability. Table 3 illustrates more details of the results.

Table 3. Summary of the simulation results between LEACH and the proposed hybrid approach based on a 10% malicious attack.

		LEACH				Proposed Hybrid Approach			
Total no of Nodes	**No. of CHs Probability**	**Max No of Rounds**	**Energy Consumption After 500 Rounds**	**Lifetime After 500 Rounds**	**Throughput**	**Max no of Rounds**	**Energy Consumption After 500 Rounds**	**Lifetime After 500 Rounds**	**Throughput**
400	0.05	2866	143.356	167	241,943	3877	142.88	180	259,207
	0.1	2331	162.71	209	193,806	3044	152.58	236	253,297
	1.15	2029	163.14	238	166,095	2950	159.0728	263	231,223
	0.2	1677	169.7	265	138,583	2900	164.17	290	209,419
	0.25	1433	173.141	275	124,194	2898	167.38	306	194,259

In addition, as shown in Figure 3a, the energy consumption was not utilized efficiently when there were 10% malicious nodes on the IoT network. The energy assumed for malicious nodes is 20 times the energy of a normal node because of the heavy requests from the attacks. Regarding this, the malicious node will broadcast its join CH message as well as its fake packets to more than one CHs, thereby disturbing the overall energy efficiency of the network. The energy consumption of the nodes can be consumed during sensing and logging. Another way possibility could be energy consumption during the sending and receiving of data.

Figure 3b shows the network lifetime of the research study. It can be observed that the network lifetime dropped significantly when there was a 10% malicious attack on the network. The outcome revealed that the network lifetime increased using the proposed hybrid approach. In addition, it could be added that the network lifetime increased with about 24% partial coverage. Table 3 also describes the results based on the existing LEACH and the proposed hybrid approach. Figure 3c shows the throughput.

As shown in Figure 3c, the study measured the throughput packets that were sent to the base station (BS). The essence of the investigation was to know how much data were transferred during a specific time via the BS. The result shows that the packets sent to the BS decreased significantly when malicious nodes (DDoS or DoS) were added to the IoT network. Furthermore, when a malicious node was behaving as a CH, the normal nodes sending packets to the CH were discarded by the malicious node, and thus the BS would not receive the packets. In the proposed hybrid approach, the malicious nodes were mitigated because of the random authorization key, as explained in the Methodology in Section 3. Figure 4 illustrates the malicious attacks based on 20% energy consumption, lifetime, and throughput to evaluate the proposed hybrid approach.

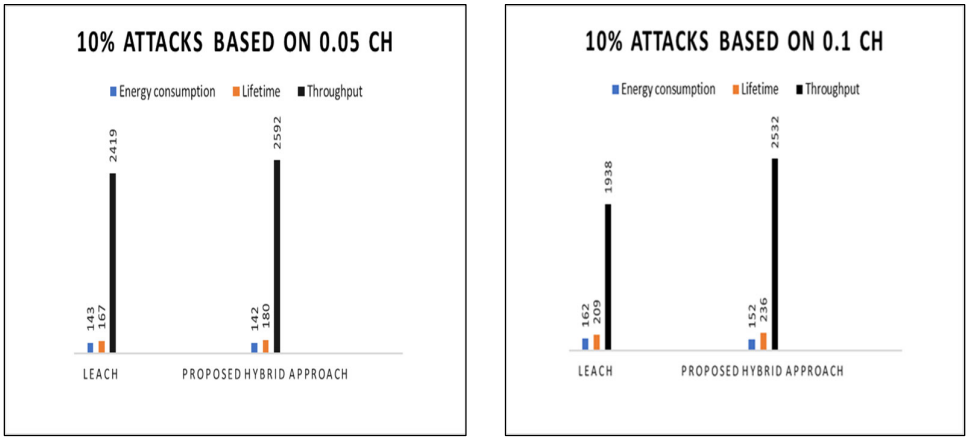
As shown in Figure 4a, the study examined the performance of IoT sensor nodes to preserve the energy of the nodes. The evaluation of the energy consumption parameter was based on 20% malicious attacks from DDoS and DoS. The output of the results based on the CHs probability, ranging from 0.05 to 0.25, was encouraging compared with the LEACH for DDoS and DoS attacks. It is proven that the proposed hybrid approach preserves more energy, even when there are attacks of 20% to the IoT environment. The detail of the comparison results is shown in Table 4. Similarly, in Figure 4b, the study also investigates the performance of the network in order to ensure that malicious attacks have no severe consequences in the IoT network. The results reveal that the proposed hybrid approach mitigates the attacks compared with the existing LEACH. Moreover, the network lifetime increased by 30% partial coverage with the 20% attacks (see Table 4). Figure 4c illustrates the throughput.

Table 4. Summary of the Simulation Results between LEACH and the proposed hybrid approach based on 20% malicious attacks.

Total no of Nodes	LEACH					Proposed Hybrid Approach			
	No. of CHs Probability	Max No of Rounds	Energy Consumption After 500 Rounds	Lifetime After 500 Rounds	Throughput	Max no of Rounds	Energy Consumption After 500 Rounds	Lifetime After 500 Rounds	Throughput
400	0.05	2060	149.48719931	166	189,260	3488	142.727979	201	254,057
	0.1	1354	162.71	210	140,760	2896	152.58	258	247,044
	1.15	1148	170.5154	239	118,739	2875	159.09	297	225,091
	0.2	1050	177.22	265	100,463	2865	164.2046	312	202,997
	0.25	978	181.0016	275	189,450	2821	167.38	327	89,835

As shown in Figure 4c, the research examines the throughput of packets sent to the base station (BS). The investigation aims to determine how much data is transmitted through the BS at any given time. This will assist the study to measure how much data will be sent if there are malicious attacks in the IoT network. The outcome reveals that the proposed hybrid approach withstands the malicious attacks of (DDoS or DoS) and the packets sent to the BS were successful within the time frame. It can be observed that in the existing LEACH their packets drop significantly due to the heavy request by the attacks. Table 4 shows the results.

Based on Table 3 the scenario indicates 10% malicious attacks to validate the proposed hybrid approach. The study analyzed the parameters such as energy consumption, lifetime, and throughput to validate the efficiency of the proposed hybrid approach. The security attacks determine by the parameters in which the more consumption of the energy the higher the request by the malicious attacks in the IoT environment. Likewise, the higher the attacks the slow of the network, and the higher the attacks the lower throughput. Besides, the study generates the CHs probability to validate each scenario of the parameters. The probability of the CHs is ranging between 0.005–0.2 to validate the proposed approach. Figure 5 provides the comparison based on LEACH 10% of malicious nodes and the proposed hybrid approach.



(**a**) (**b**)

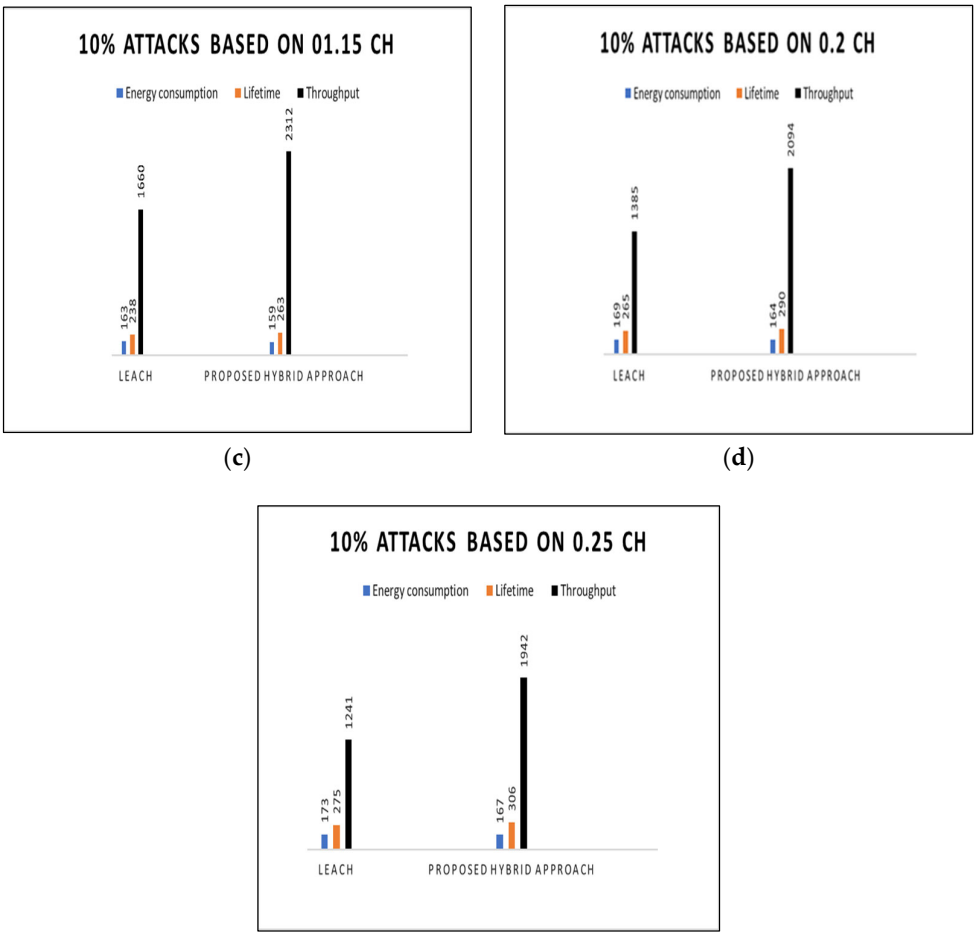


Figure 5. Attacks based on (**a**) 0.05 CH, (**b**) 0.1 CH, (**c**) 01.15 CH, (**d**) 0.2 CH, and (**e**) 0.25 CH.

The study selected 0.05 to 0.25 CHs, based on Table 3, and compared the findings based on the energy consumption, lifetime, and throughput of the existing LEACH and proposed hybrid approached. As shown in Figure 5a–e, the spectral rations and predominant periods for both parameters were encouraging based on the proposed approach compared with the existing LEACH approach. It is evident that the proposed hybrid approach consumed less energy and improved the lifetime of the network and the throughput. Figure 6 provides the comparison based on the LEACH approach and the proposed hybrid approach for 20% malicious nodes. Table 4 summarizes the simulation results for the LEACH approach and the proposed hybrid approach for 20% malicious nodes.

Based on the comparison in Figure 6, the study selected the 0.05 to 0.25 CHs probability, as depicted in Table 4 above. The comparison revealed that the existing LEACH approach decreased when there were 20% malicious nodes for the parameters. The result in Figure 6a,b shows the comparison between the three parameters for energy consumption, lifetime, and throughput. The comparison indicates that the proposed hybrid approach consumes less energy and enhances the lifetime and throughput when compared with the existing LEACH approach.

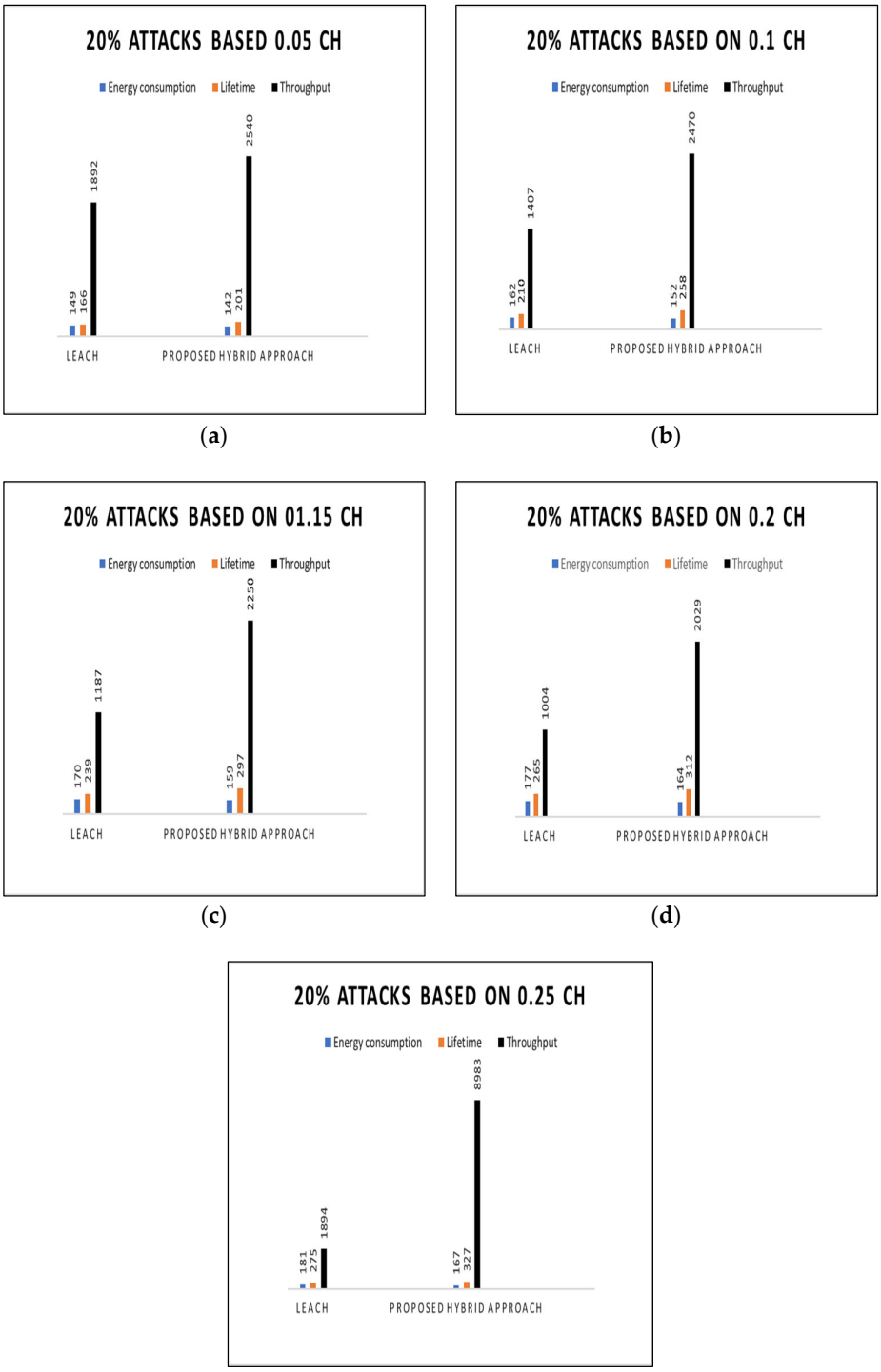


Figure 6. Attacks based on (**a**) 0.05 CH, (**b**) 0.1 CH, (**c**) 01.15 CH, (**d**) 0.2 CH, and (**e**) 0.25 CH.

5. Conclusions

In the last years, IoT has undergone various attacks by intruders because of the poor design of methods for mitigating malicious attacks such as DDoS and DoS. Additionally, the lack of robust security protection has motivated intruders to perform a series of attacks on the IoT network and its devices. These attacks lead to data exfiltration and financial

losses. The study performs a rigorous investigation and further proposes a robust framework that withstands the cybersecurity attacks of DDoS and DoS in the IoT environment. The study believes that the proposed solution can also help future researchers to tackle the expansion of data exfiltration caused by DDoS and DDoS attacks in the IoT environment. In essence, the experimental results show that the proposed hybrid approach prevents data exfiltration caused by DDoS and DoS attacks by about 95.4%, and shows average network lifetime, energy consumption, and throughput improvements of about 15%, 25%, and 60%, respectively.

Author Contributions: The authors contributed to the entire manuscript. A.A.G. performed the simulation and manuscript writing. R.A. supervised the work. H.A. reviewed and edited the manuscript. All authors have read and agreed to the published version of the manuscript.

Funding: This publication is part of research work supported by Universiti Teknologi PETRONAS through Yayasan UTP (YUTP) with grant (No: 015LC0-104).

Data Availability Statement: Data sharing not applicable. No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Acknowledgments: The authors acknowledge the Centre of Graduate Studies (CGS) for the support and encouragement during the study. The authors also express their gratitude to Universiti Teknologi PETRONAS and YUTP for the financial support, which made the research possible.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Peerbits, 10 Biggest Security Challenges for IoT, Blog. Available online: https://www.peerbits.com/blog/biggest-iot-security-challenges.html (accessed on 15 March 2021).
2. Lee, I. The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. *Internet Things* **2019**, *7*, 100078, doi:10.1016/j.iot.2019.100078.
3. Wortmann, A.-P.D.F.; Flüchter, K. Internet of Things. *Bus. Inf. Syst. Eng.* **2015**, *57*, 221–224, doi:10.1007/s12599-015-0383-3.
4. Government information quarterly. *Gov. Inf. Q.* **2001**, *18*, 375–378, doi:10.1016/s0740-624x(01)00093-4.
5. Cooper, K. Security for the Internet of Things. Master Thesis, KTH Royal Instituteof Technology and Technical University of Denmark, Lyngby, Denmark, 26 June 2015.
6. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* **2018**, *38*, 8–27, doi:10.1016/j.jisa.2017.11.002.
7. Mocrii, D.; Chen, Y.; Musilek, P. IoT-based smart homes: A review of system architecture, software, communications, privacy and security. *Internet Things* **2018**, *1–2*, 81–98, doi:10.1016/j.iot.2018.08.009.
8. Mainetti, L.; Patrono, L.; Vilei, A. Evolution of wireless sensor networks towards the Internet of Things: A survey. In Proceedings of the SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks, Split, Croatia, 15–17 September 2011; pp. 16–21.
9. Ghali, H.S.A.; Ahmad, A.A.; Alhussian, R. Comparative Analysis of DoS and DDoS Attacks in Internet of Things Environment. In Proceedings of the CSOC 2020: Artificial Intelligence and Bioinspired Computational Methods, Zlin, Czech Republic, 15 July 2020; pp. 183–194.
10. Liagkou, V.; Kavvadas, V.; Chronopoulos, S.K.; Tafiadis, D.; Christofilakis, V.; Peppas, K.P. Attack Detection for Healthcare Monitoring Systems Using Mechanical Learning in Virtual Private Networks over Optical Transport Layer Architecture. *Computers* **2019**, *7*, 24, doi:10.3390/computation7020024.
11. Jing, Q.; Vasilakos, A.V.; Wan, J.; Lu, J.; Qiu, D. Security of the Internet of Things: Perspectives and challenges. *Wirel. Net.* **2014**, *20*, 2481–2501, doi:10.1007/s11276-014-0761-7.
12. Patel, C.; Doshi, N. Security Challenges in IoT Cyber World. In Proceedings of the International Conference TRANSBALTICA, Vilnius, Lithuania, 2–3 May 2019; pp. 171–191.
13. Yaqoob, I.; Hashem, I.A.T.; Ahmed, A.; Kazmi, S.A.; Hong, C.S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Futur. Gener. Comput. Syst.* **2019**, *92*, 265–275, doi:10.1016/j.future.2018.09.058.
14. Jazi, H.H.; Gonzalez, H.; Stakhanova, N.; Ghorbani, A.A. Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. *Comput. Networks* **2017**, *121*, 25–36, doi:10.1016/j.comnet.2017.03.018.
15. Smith, T.; Aznarez, O.; Tsarou, A. The Dangers of Underestimating DDoS Attacks. Available online: https://www.corero.com/blog/the-dangers-of-underestimating-ddos-attacks/ (accessed on 4 February 2021).
16. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015.

17. Harbi, Y.; Aliouat, Z.; Harous, S.; Bentaleb, A.; Refoufi, A. A Review of Security in Internet of Things. *Wirel. Pers. Commun.* **2019**, *108*, 325–344, doi:10.1007/s11277-019-06405-y.
18. Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28, doi:10.1016/j.jnca.2017.04.002.
19. Sfar, A.R.; Natalizio, E.; Challal, Y.; Chtourou, Z. A roadmap for security challenges in the Internet of Things. *Digit. Commun. Net.* **2018**, *4*, 118–137, doi:10.1016/j.dcan.2017.04.003.
20. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A Survey. J. *Comput. Netw.* **2010**, *54*, 2787–2805. doi:10.1016/j.comnet.2010.05.010.
21. De Saint-Exupery, A. Internet of Things. Available online: https://docplayer.net/11937485-Internet-of-things-strategic-research-roadmap-antoine-de-saint-exupery.html (accessed on 25 October 2020).
22. Said, O. Accurate Performance Evaluation of Internet Multicast Architectures: Hierarchical and Fully Distributed vs. Service-Centric/ KSII Trans. *Internet Inf. Syst.* **2013**, *7*, 2194–2212.
23. Farooq, M.U.; Waseem, M.; Khairi, A.; Mazhar, S. A Critical Analysis on the Security Concerns of Internet of Things (IoT). *Int. J. Comput. Appl.* **2015**, *111*, 1–6, doi:10.5120/19547-1280.
24. . Mamoon, Q.; Habaebi, M.H. Journal of Network and Computer Applications Autonomic schemes for threat mitigation in Internet of Things. *J. Netw. Comput. Appl.* **2015**, *49*, 112–127.
25. Aldaej, A. Enhancing Cyber Security in Modern Internet of things (IoT) Using Intrusion Prevention Algorithm for IoT (IPAI). *IEEE Access* **2019**, 1, doi:10.1109/access.2019.2893445.
26. Pa, Y.M.P.; Suzuki, S.; Yoshioka, K.; Matsumoto, T.; Kasama, T.; Rossow, C. IoTPOT: A Novel Honeypot for Revealing Current IoT Threats. *J. Inf. Process.* **2016**, *24*, 522–533, doi:10.2197/ipsjjip.24.522.
27. Lu, Y.; Da Xu, L. Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics. *IEEE Internet Things J.* **2018**, *6*, 2103–2115, doi:10.1109/jiot.2018.2869847.
28. Miorandi, D.; Sicari, S.; De Pellegrini, F.; Chlamtac, I. Ad Hoc Networks Internet of things: Vision. *Appl. Res. Challeng.* **2012**, *10*, 1497–1516.
29. Islam, J.; Rahman, A.; Kabir, S.; Karim, R.; Acharjee, U.K.; Nasir, M.K.; Band, S.S.; Mosavi, A. Blockchain-SDN Based Energy Optimized and Distributed Secure Architecture for IoTs in Smart Cities. *Preprints* **2020**, 1–20, doi:10.20944/preprints202011.0552.v1.
30. El Saadawy, M.; Shaaban, E. Enhancing S-LEACH security for wireless sensor networks. In Proceedings of the IEEE International Conference Electro. *Inf. Technol.* **2012**, 1–6, doi:10.1109/eit.2012.6220698.
31. Behera, T.M.; Samal, U.C.; Mohapatra, S.K. Energy-efficient modified LEACH protocol for IoT application. *IET Wirel. Sens. Syst.* **2018**, *8*, 223–228, doi:10.1049/iet-wss.2017.0099.
32. Zhang, G.-A.; Gu, J.-Y.; Bao, Z.-H.; Xu, C.; Zhang, S.-B. Joint routing and channel assignment algorithms in cognitive wireless mesh networks. *Trans. Emerg. Telecommun. Technol.* **2012**, *25*, 294–307, doi:10.1002/ett.2560.
33. Ibrahim, M.H. Octopus: An edge-fog mutual authentication scheme. *Int. J. Netw. Secur.* **2016**, *18*, 1089–1101.