


Article

# Performance Evaluation and Validation of QCM (Query Control Mechanism) for QoS-Enabled Layered-Based Clustering for Reactive Flooding in the Internet of Things

Fawad Ali Khan <sup>1,\*</sup>, Rafidah Md Noor <sup>1,2,\*</sup>, Miss Laiha Mat Kiah <sup>1</sup>, Ismail Ahmedy <sup>1</sup> , Mohd Yamani Idna Idris <sup>1</sup>, Tey Kok Soon <sup>1</sup> and Muneer Ahmad <sup>3</sup>

<sup>1</sup> Department of Computer System & Technology, Faculty of Computer Science & Information Technology, University Malaya, Kuala Lumpur 50603, Malaysia; misslaiha@um.edu.my (M.L.M.K.); ismailahmedy@um.edu.my (I.A.); yamani@um.edu.my (M.Y.I.I.); koksoon@um.edu.my (T.K.S.)

<sup>2</sup> Centre for Mobile Cloud Computing Research (C4MCCR), Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur 50603, Malaysia

<sup>3</sup> Department of Information System, Faculty of Computer Science & Information Technology, University Malaya, Kuala Lumpur 50603, Malaysia; mmalik@um.edu.my

\* Correspondence: fawadkn@siswa.um.edu.my (F.A.K.); fidah@um.edu.my (R.M.N.)

Received: 25 September 2019; Accepted: 8 November 2019; Published: 3 January 2020



**Abstract:** Internet of Things (IoT) facilitates a wide range of applications through sensor-based connected devices that require bandwidth and other network resources. Enhancement of efficient utilization of a heterogeneous IoT network is an open optimization problem that is mostly suffered by network flooding. Redundant, unwanted, and flooded queries are major causes of inefficient utilization of resources. Several query control mechanisms in the literature claimed to cater to the issues related to bandwidth, cost, and Quality of Service (QoS). This research article presented a statistical performance evaluation of different query control mechanisms that addressed minimization of energy consumption, energy cost and network flooding. Specifically, it evaluated the performance measure of Query Control Mechanism (QCM) for QoS-enabled layered-based clustering for reactive flooding in the Internet of Things. By statistical means, this study inferred the significant achievement of the QCM algorithm that outperformed the prevailing algorithms, i.e., Divide-and-Conquer (DnC), Service Level Agreements (SLA), and Hybrid Energy-aware Clustering Protocol for IoT (Hy-IoT) for identification and elimination of redundant flooding queries. The inferential analysis for performance evaluation of algorithms was measured in terms of three scenarios, i.e., energy consumption, delays and throughput with different intervals of traffic, malicious mote and malicious mote with realistic condition. It is evident from the results that the QCM algorithm outperforms the existing algorithms and the statistical probability value “P” < 0.05 indicates the performance of QCM is significant at the 95% confidence interval. Hence, it could be inferred from findings that the performance of the QCM algorithm was substantial as compared to that of other algorithms.

**Keywords:** QoS; redundant query; Internet of things; network flooding; energy efficiency

## 1. Introduction

The Internet of Things (IoT) has become quite famous in the recent years in that many of our daily routine devices are being connected with us, covering many capabilities such as sensing, autonomy, and contextual awareness [1]. The IoT, resulting from Internet progress and the innovative evolution of smart devices, has led to the development of new computing prototypes. IoT is the next revolutionary technology that converts the present communication infrastructure into a completely

futuristic network [2]. IoT is expected to contain high numbers of sensors collecting and passing on data on environmental conditions, physiological measurements, machine operational data, etc. IoT provides an integration of various sensors and objects that could communicate directly with one another without human intervention [3,4]. The primary purpose of the IoT is to allow secure data exchange between the real world devices and applications [5–7].

IoT promises a smart environment that would save time, energy, good quality of service (QoS), resources, and there will be less delay as compared to traditional wireless sensor networks [8]. Dynamic resource scheduling for heterogeneous workloads in IoT is critical to ensure QoS, level of energy consumptions on each mote, and traffic delay during data transmission [9]. Energy consumptions, QoS, and delay are the major challenging requirements for IoT networks, since data transmission in IoT network is based on priority [10–16]. Reference [17] proposed an adaptive meta-heuristic search for redundancy in IoT networks using the AntClust technique. Reference [18] used process-querying techniques to develop an enabling business intelligence for resource-constrained devices. Reference [19] proposed a scalability mechanism for IoT devices. Since scalability has become an important aspect that needs to be considered in any IoT system, the proposed mechanism enables IoT devices to be adaptable to environmental change. In addition, a three-level framework for IoT redundancy control was proposed by [20]. Reference [21] used a divide-and-conquer (DnC) method to develop an approach for improving energy efficiency in QoS-constrained WSNs (wireless sensor networks). Reference [22] proposed a node-level energy efficiency protocol for IoT devices to improve the energy efficiency in an IoT network. Reference [23] proposed a QoS architecture for IoT and cloud computing platforms to enable public/users to have easy access over diversified smart applications and services, distributed in the cloud with one IoT-enabled Intelligent Smart Card (ISC), through mobile devices with assured quality of service. In addition, modeling QoS in IoT applications was proposed by [24]. Reference [25] discussed network architecture and QoS issues in the IoT for a smart city. Reference [26] proposed a discrete component circuit implementation model together with its computational simulations using Bouali's system.

The primary purpose of the IoT is to allow secure data exchange between the real world devices and applications [27–29]. It is a known fact that IoT has the potential for a wide range of applications relating to agriculture, transportation, health, education, supply chain, farming, plant disease diagnosis, poultry, irrigation, and pest control [30,31]. Each application requires many sensors to connect and communicate with another, which may reduce the QoS of the network due to inefficient resource utilization, traffic delay due to redundant messages/queries because each device has direct access to cloud resources and energy consumption [32,33]. Layered-based system model with different motes communicating redundantly in IoT is illustrated in Figure 1 [34].

IoT is therefore based upon the integration of several communication solutions, identification and tracking technologies, sensor and actuator networks and distributed smart objects [33]. These objects/devices are connected to each other and share the same network for communicating with each other. All the devices are connected with the sensor to detect the particular surrounding conditions and analyze the situation and work accordingly. IoT devices are also programmed to take a decision automatically [34], according to the user so that the user can make the best decision. This interconnected network can bring lot of advancement in the technology of application and services that can bring economic benefit to the global business development. Many devices are connected to the internet to share local information in cyberspace [35–37].

Figure 1 shows the system model with different sensor motes communicating with each other between the physical (sensor) and network layers of IoT. From the figure, it can be seen that redundant messages, unwanted queries and network flooding are the major causes of inefficient utilization of resources, thus resulting in IoT devices consuming more energy with a high computational time (i.e., delay in data transmission), which in turn affects the network QoS [4]. Moreover, solving these issues in IoT networks is demanding due to the constraint nature of the devices with limited energy.

Presently, to the best of our knowledge, no mechanisms for identification of redundant queries have been developed in this domain.

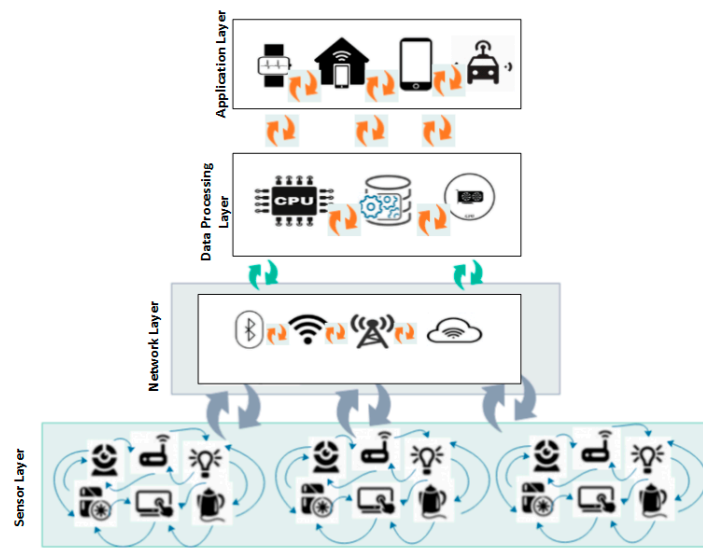


Figure 1. Layered-based system model with different motes communicating redundantly in IoT.

We examine several approaches for tackling unwanted and redundant communication in IoT networks to enable us to understand the sequence of actions that take place when flooding happens and propose a Cluster-Based Flooding (CBF) technique. The proposed technique is an interoperable solution both for physical layer and network layer devices. CBF divides the network into different clusters; local queries information are proactively maintained by the Intralayer clustering (IALC), while Interlayer clustering (IELC) is responsible for reactively obtaining the routing queries to the destinations outside the cluster. CBF is a hybrid approach, having the potential to be more efficient than traditional schemes in term of query traffic generation.

A QoS-enabled QCM model is developed, and the results of the simulation show the superior performance against state of the art approaches in terms of traffic delay, QoS throughput, and energy consumption, under various performance metrics compared with traditional flooding and state of the art. In order to figure out real understanding of flooding in IoT networks, we provide modeling of the redundant queries which leads to flooding in Figure 2 [34].

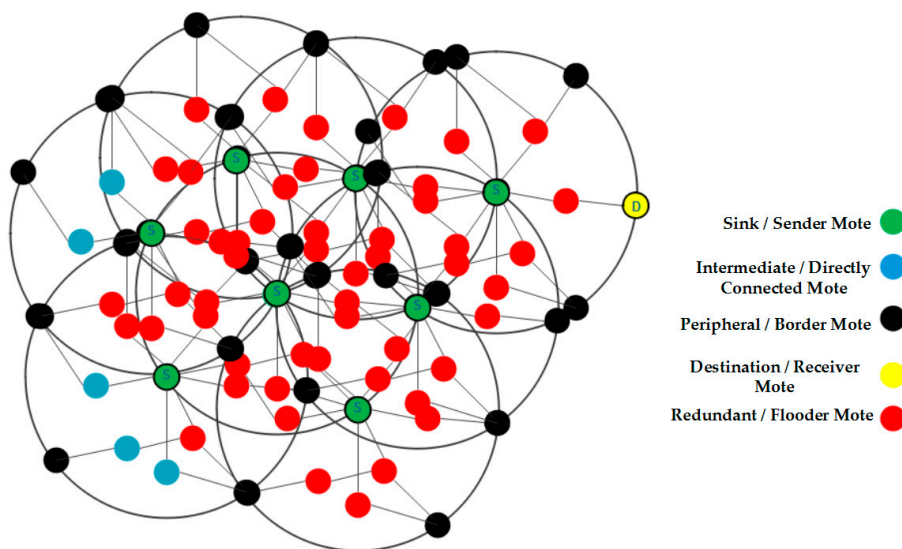


Figure 2. Flooding as a result of redundant queries.

## 2. Motivation

The Internet of Things has gained substantial attention over the last few years because of connecting daily things in a wide range of application and domains. Many sensors require bandwidth and network resources to give-and-take queries among heterogeneous IoT networks. The network sometimes becomes unable to handle unwanted and redundant queries generated from different smart devices. In addition, the network is also not able to prioritize the important queries among flooded queries. This research developed a new query control mechanism that could manage priority queries and refrain redundant and unwanted queries. This idea was able to save time and resources of networks with an efficient query management. Further, the performance evaluation of such query control mechanisms required inferential analysis of simulated results to statistically validate the performance parameters of QCMs under discussion.

## 3. Problem Statement

Network flooding is a key questioning strategy for successful exchange of queries. However, the risk of the original flooding is prone to unwanted and redundant network queries which may lead to cause heavy network traffic. Redundant, unwanted and flooded queries are the major cause of inefficient utilization of resources. IoT devices consume more energy and high computational time as compare to wireless sensor networks [15]. More queries lead to consumption of bandwidth, increase cost, and degrade QoS. Current existing approaches focus primarily on how to speed up the basic routing for IoT devices. However, solutions for flooding are not being addressed. This research proposed a new query control mechanism and evaluated its performance by statistical means.

## 4. Methodology

This research is based on the hypothesis that the proposed **QCM (Query Control Mechanism)** algorithm (Khan, F. A., Noor, R. M., Mat Kiah, M. L., Noor, N. M., Altowajri, S. M., & Rahman, A. U., 2019) outperforms the other existing algorithms, i.e., DnC, SLA, and Hy-IoT for QoS-enabled layered-based clustering for reactive flooding in the Internet of Things. Table 1 presents the important illustration of symbols and abbreviations used this the methodology.

**Table 1.** Illustration of symbols and notations used in the manuscript.

Symbol or Notation	Meaning
$H_0$	Null Hypothesis
$H_1$	Alternative Hypothesis
$\mu$	Mean of sample values
DnC	Divide-and-Conquer method
SLA	Service-Level Agreements
Hy-IoT	Hybrid energy aware clustered protocol for IoT heterogeneous network
QoS	Quality of Service
$S_D$	Standard Deviation
$\Sigma$	Summation of a data series
MSR	Mean squares for samples
MSE	Mean squares for errors
SSR	Sum of squares for samples
SSE	Sum of squares for errors
QCM	Query control mechanism
P	Probability

The research considered the following two hypotheses for inferential analysis,

1. Null hypothesis  $H_0$  ( $\mu_2 - \mu_1 = 0$ ): There is no statistical significance of results between the proposed **QCM** algorithm and other existing algorithms (DnC, SLA, and Hy-IoT) for QoS-enabled layered-based clustering for reactive flooding in the Internet of Things.
2. Alternative hypothesis  $H_1$  ( $\mu_2 - \mu_1 > 0$ ): There is statistical significant relationship between the proposed **QCM** algorithm and other existing algorithms (DnC, SLA, and Hy-IoT) for QoS-enabled layered-based clustering for reactive flooding in the Internet of Things.

Further, the researcher performed a T-test and an ANOVA test for the above hypothesis testing. Let the Sample mean difference be

$$\bar{d} = \mu_2 - \mu_1 \quad (1)$$

where  $\mu_1$  is the sample mean of the data set of results for the first algorithm and  $\mu_2$  is the sample mean of the data set of results for the second comparable algorithm.

Sample standard deviation

$$S_D = \sqrt{\frac{1}{N-1} \sum_{i=1}^N (x_i - \bar{d})^2} \quad (2)$$

Here, data points are  $x_1, x_2, x_3, \dots, x_N$  in the data sets of results of the two comparable algorithms.

Paired Sample T-test:

$$T = \frac{\bar{d} - 0}{S_D / \sqrt{n}} \quad (3)$$

Here,  $n$  represents the number of observations. We find the probability value ( $p$ ) by observing the test statistics under the null and alternative hypothesis. This probability would help to identify the magnitude of the significance in the results for our proposed **QCM** algorithm.

The test calculates the probability value (P-value) based on the data sets of the results for different comparable algorithms. The standard confidence interval is 0.05 (95% confidence interval); P-values less than 0.05 are considered statistically significant. On the contrary, P-values larger than the chosen confidence interval infer that performances of comparable algorithms have no statistical significance and hence no algorithm outperformed the other algorithms in this comparison.

In addition, the authors performed an "ANOVA test" [35–37] to validate the performance measure of algorithms. The ANOVA test contains the following features,

Mean square for samples,

$$MSR = \frac{SSR}{k-1} \quad (4)$$

Similarly, the mean square for error,

$$MSE = \frac{SSE}{n-k} \quad (5)$$

Now the F statistics becomes

$$F = \frac{MSR}{MSE} \quad (6)$$

This research, by statistical means, evaluates the performance of different QoS-enabled layered-based clustering algorithms for reactive flooding in the Internet of Things with the following measures.

1. **Inferential analysis in terms of Energy Consumption**
  - a. Energy consumption with different intervals of traffic
  - b. Energy consumption with malicious mote
  - c. Energy consumption with malicious mote with a realistic condition
2. **Inferential analysis in terms of Delay**

- a. Delay with different intervals of traffic
- b. Delay with malicious mote
- c. Delay with malicious mote with a realistic condition

### 3. Inferential analysis in terms of Throughput

- a. Throughput with different intervals of traffic
- b. Throughput with malicious mote
- c. Throughput with malicious mote with a realistic condition

Based on our hypothesis theories stated above, we find the probability value “P” employing the statistical t-test to figure out acceptance or rejection of our Null hypothesis (or alternative hypothesis) as a metric for performance evaluation of proposed and existing algorithms.

## 5. Results

The performance estimation and evaluation of the proposed technique against up-to-date DnC, SLA [2,3] and Hy-IoT [32] methods for tracing and mitigating the unwanted and redundant reactive flooding are described in this section. Routing protocol and MDP protocol [24] are ad-hoc routing and Contiki, respectively. To obtain the appropriate results, simulation is performed 60 times based on the following three scenarios.

- Scenario based on varied intervals of traffic: This condition plays an important role to gauge and ensure the effectiveness of flooding attacks and to regulate the defensive techniques in varying intervals of traffic. The range for the traffic interval is set as (1 s to 10 s), where 1 s is faster and 10 s is slower.
- Scenario based on a varied number of mischievous motes: this condition is favorable in analyzing the impact of a flooding attack on the network and to take the appropriate action to counter mischievous motes. Motes (2,6,10,15) are set as mischievous motes, and the interval of traffic is set to (1 s) where 1 s is referred as the fastest traffic in the network.
- Condition based on realistic scenario: In this conditional scenario, motes are restricted to not transfer the route query information simultaneously; they are only allowed to transfer route query requests at different intervals of time. These intervals are randomly set from 1 s to 10 s.

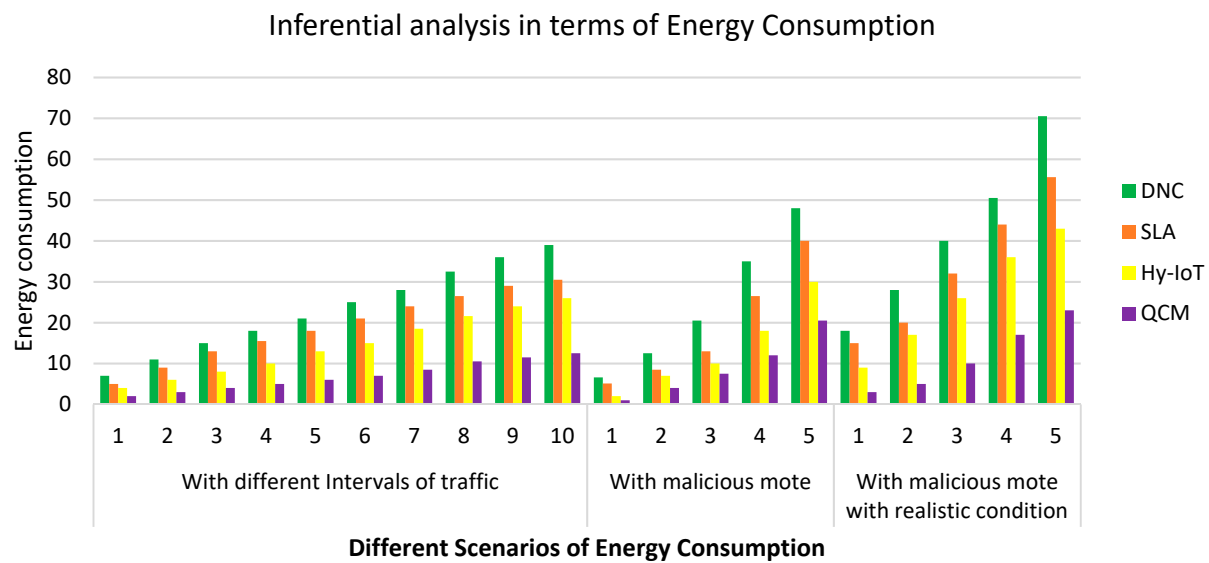
Further, this section describes the inferential analysis of experimental results related to the performance evaluation and validation of the proposed **QCM (Query Control Mechanism)** algorithm (Khan, F. A., Noor, R. M., Mat Kiah, M. L., Noor, N. M., Altowaijri, S. M., & Rahman, A. U., 2019). We present here the rejection of the Null hypothesis and acceptance of the alternative hypothesis since the **QCM** algorithm outperforms (95% confidence interval) the existing algorithms, i.e., DnC, SLA, and Hy-IoT for QoS-enabled layered-based clustering for reactive flooding in the Internet of Things.

#### Case 1: Inferential analysis in terms of energy consumption

Here, in this case, we discuss the performance evaluation in terms of energy consumption with three different scenarios, i.e., different intervals of traffic, malicious mote and malicious mote with realistic conditions.

Figure 3 depicts energy consumptions with respect to different scenarios, i.e., different intervals of traffic, with malicious mote and with malicious mote and with realistic conditions. The proposed QCM technique outperformed DnC, SLA, and Hy-IoT approaches in term of dropping the average consumption of energy. Because the proposed technique is capable of detecting flooder motes and detaching them from the network, this reduces the level of energy consumption that arises during redundant and unwanted flooding attacks, whereas the average energy consumption of DnC and SLA is approximately 21 and 18%, respectively, from (1 to 5) seconds of intervals, and this ratio continuously rises as the interval increases. However, in the case of the proposed mechanism, the ratio of the consumption of energy falls to 6% as compared to 13% in the existing Hy-IoT approach.





**Figure 3.** Energy Consumption with respect to different scenarios.

We can observe that **QCM** achieves the lowest energy consumption as compared to other prevailing algorithms in the described scenarios.

Table 2 presents the statistical observations of data related to the inferential analysis of **QCM** and other existing algorithms. We can see that the statistical significant value **P** is less than our chosen confidence interval of 0.05 which is evidence that our proposed **QCM** algorithm outperforms the existing algorithms. Hence, the Null hypothesis is rejected and **QCM** achieves the significant prediction value in the desired confidence interval.

**Table 2.** Inferential analysis of the proposed **QCM** algorithm in terms of energy consumption scenarios.

<b>“Energy consumption” with different intervals of traffic</b>			
<i>Statistics</i>	<i>QCM and DNC</i>	<i>QCM and SLA</i>	<i>QCM and Hy-IoT</i>
Pearson Correlation	0.995898024	0.985945791	0.998690321
t Stat	−7.234140089	−7.658424991	−5.902772999
<b>P (T ≤ t) one-tail</b>	<b>0.000024</b>	<b>0.000016</b>	<b>0.000114</b>
t Critical one-tail	1.833112933	1.833112933	1.833112933
<b>P (T ≤ t) two-tail</b>	<b>0.000049</b>	<b>0.000031</b>	<b>0.000228</b>
t Critical two-tail	2.262157163	2.262157163	2.262157163
<b>“Energy consumption” with malicious mote</b>			
<i>Statistics</i>	<i>QCM and DNC</i>	<i>QCM and SLA</i>	<i>QCM and Hy-IoT</i>
Pearson Correlation	0.991199989	0.990539256	0.997641141
t Stat	−3.69153586	−3.080170745	−2.910781287
<b>P (T ≤ t) one-tail</b>	<b>0.010495227</b>	<b>0.018462731</b>	<b>0.021822006</b>
t Critical one-tail	2.131846786	2.131846786	2.131846786
<b>P (T ≤ t) two-tail</b>	<b>0.020990453</b>	<b>0.036925463</b>	<b>0.043644012</b>
t Critical two-tail	2.776445105	2.776445105	2.776445105
<b>“Energy consumption” with malicious mote with realistic conditions</b>			
<i>Statistics</i>	<i>QCM and DNC</i>	<i>QCM and SLA</i>	<i>QCM and Hy-IoT</i>
Pearson Correlation	0.988654058	0.997737729	0.985054247
t Stat	−5.47596162	−5.744022068	−5.700342309
<b>P (T ≤ t) one-tail</b>	<b>0.002706491</b>	<b>0.002276306</b>	<b>0.002340359</b>
t Critical one-tail	2.131846786	2.131846786	2.131846786
<b>P (T ≤ t) two-tail</b>	<b>0.005412981</b>	<b>0.004552613</b>	<b>0.004680719</b>
t Critical two-tail	2.776445105	2.776445105	2.776445105

An exact realistic analysis of QCM is conducted to find the level of mischievous motes during flooding expansion in the network. It is evident from the result that in the presence of malicious motes, the level of energy consumption increases gradually. At malicious mote 2, the levels of energy consumption are approximately (8 and 5%) for DnC and SLA approaches respectively, and at malicious mote 15, this consumption level reaches approximately (48 and 40%). Hence, by introducing QCM, this level falls to approximately (2, 4, and 20%) at malicious mote (2, 6 and 15), respectively.

Table 3 presents the ANOVA test statistics of the proposed QCM algorithm compared with other algorithms. We can find here that “F statistics” values are sufficiently larger than “F critical values”. In addition, the “P values” are less than 0.05, which achieves our 95% confidence interval, showing that the proposed QCM algorithm outperforms the existing algorithms evaluated through inferential analysis.

**Table 3.** ANOVA statistics of the proposed QCM algorithm in terms of energy consumption scenarios.

<b>“Energy consumption” with different intervals of traffic</b>						
<i>Source of Variation</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-value</i>	<i>F crit</i>
Between Groups	1454.17075	3	484.7235833	7.408406	0.000547983	2.866265551
Within Groups	2355.439	36	65.42886111			
Total	3809.60975	39				
<b>“Energy consumption” with malicious mote</b>						
<i>Source of Variation</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-value</i>	<i>F crit</i>
Between Groups	673.1095	3	224.3698333	4.334246	0.029824869	3.238871517
Within Groups	2690.596	16	168.16225			
Total	3363.7055	19				
<b>“Energy consumption” with malicious mote with realistic conditions</b>						
<i>Source of Variation</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-value</i>	<i>F crit</i>
Between Groups	2399.974	3	799.9913333	3.349041	0.04550264	3.238871517
Within Groups	3821.948	16	238.87175			
Total	6221.922	19				

### Case 2: Inferential analysis in terms of Delay

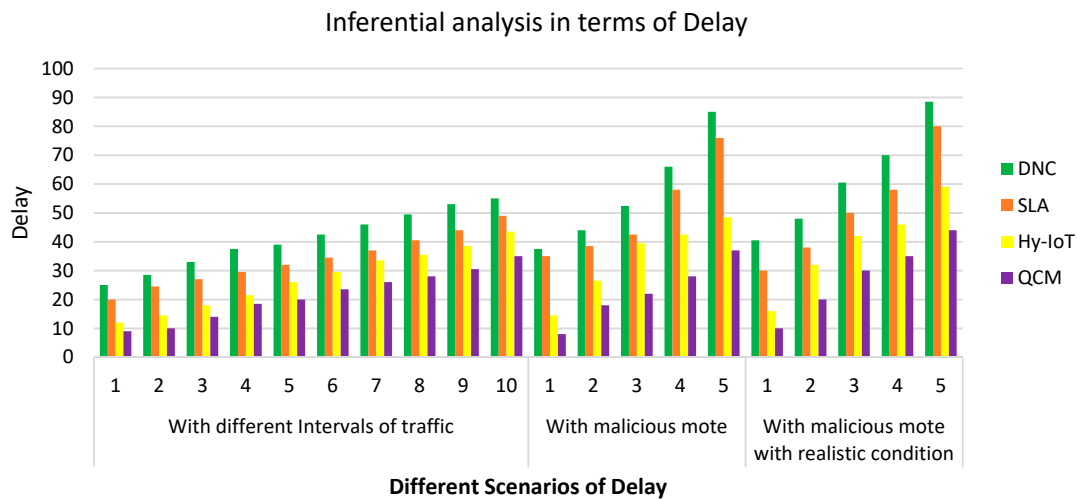
The effect of traffic delay on the number of malicious motes, the time interval and malicious motes under realistic conditions are described in this section. QCM outperformed DnC, SLA and Hy-IoT by having the least traffic delays. QCM has the ability to detect, pause and detach the flooding mote from the network, which helped in improving its performance. On the other hand, the redundant and unwanted queries were also removed by detaching the flooding motes.

Here, in this case, we discuss the performance evaluation in terms of delay with three different scenarios, i.e., different intervals of traffic, malicious mote and malicious mote with realistic conditions.

Figure 4 presents the “delay” with respect to different scenarios, i.e., different intervals of traffic, with malicious mote and with malicious mote and with realistic conditions. We can observe that QCM achieves the lowest delay as compared to other prevailing algorithms in described scenarios.

Table 4 presents the statistical observations of data related to the inferential analysis of QCM and other existing algorithms. We can see that the statistical significance value **P** is less than our chosen confidence interval 0.05 which is evidence that our proposed QCM algorithm outperforms the existing algorithms. Hence, the Null hypothesis is rejected and QCM achieves the significant prediction value in the desired confidence interval.





**Figure 4.** Delay with different intervals of traffic.

**Table 4.** Inferential analysis of the proposed QCM algorithm in terms of “delay” scenarios.

“Delay” with different intervals of traffic			
<i>Statistics</i>	<i>QCM and DNC</i>	<i>QCM and SLA</i>	<i>QCM and Hy-IoT</i>
Pearson Correlation	0.994443621	0.988982601	0.996492201
t Stat	−35.04330697	−28.82155963	−8.856366815
<b>P (T ≤ t) one-tail</b>	<b>0.000000</b>	<b>0.000000</b>	<b>0.000005</b>
t Critical one-tail	1.833112933	1.833112933	1.833112933
<b>P (T ≤ t) two-tail</b>	<b>0.000000</b>	<b>0.000000</b>	<b>0.000010</b>
t Critical two-tail	2.262157163	2.262157163	2.262157163
“Delay” with malicious mote			
<i>Statistics</i>	<i>QCM and DNC</i>	<i>QCM and SLA</i>	<i>QCM and Hy-IoT</i>
Pearson Correlation	0.971603496	0.941343288	0.960608021
t Stat	−8.753903055	−7.964645156	−5.894374846
<b>P (T ≤ t) one-tail</b>	<b>0.000469295</b>	<b>0.000673192</b>	<b>0.002071644</b>
t Critical one-tail	2.131846786	2.131846786	2.131846786
<b>P (T ≤ t) two-tail</b>	<b>0.00093859</b>	<b>0.001346383</b>	<b>0.004143289</b>
t Critical two-tail	2.776445105	2.776445105	2.776445105
“Delay” with malicious mote with realistic conditions			
<i>Statistics</i>	<i>QCM and DNC</i>	<i>QCM and SLA</i>	<i>QCM and Hy-IoT</i>
Pearson Correlation	0.978790154	0.971228078	0.994541157
t Stat	−11.51506032	−7.200852222	−7.656162383
<b>P (T ≤ t) one-tail</b>	<b>0.000162379</b>	<b>0.00098563</b>	<b>0.000782041</b>
t Critical one-tail	2.131846786	2.131846786	2.131846786
<b>P (T ≤ t) two-tail</b>	<b>0.000324759</b>	<b>0.001971259</b>	<b>0.001564082</b>
t Critical two-tail	2.776445105	2.776445105	2.776445105

Table 5 presents the ANOVA test statistics of the proposed QCM algorithm compared with other algorithms. We can find here that “F statistics” values are sufficiently larger than “F critical values”. In addition, the “P values” are less than 0.05, which achieves our 95% confidence interval, showing that the proposed QCM algorithm outperforms the existing algorithms evaluated through inferential analysis.

### Case 3: Inferential analysis in terms of throughput

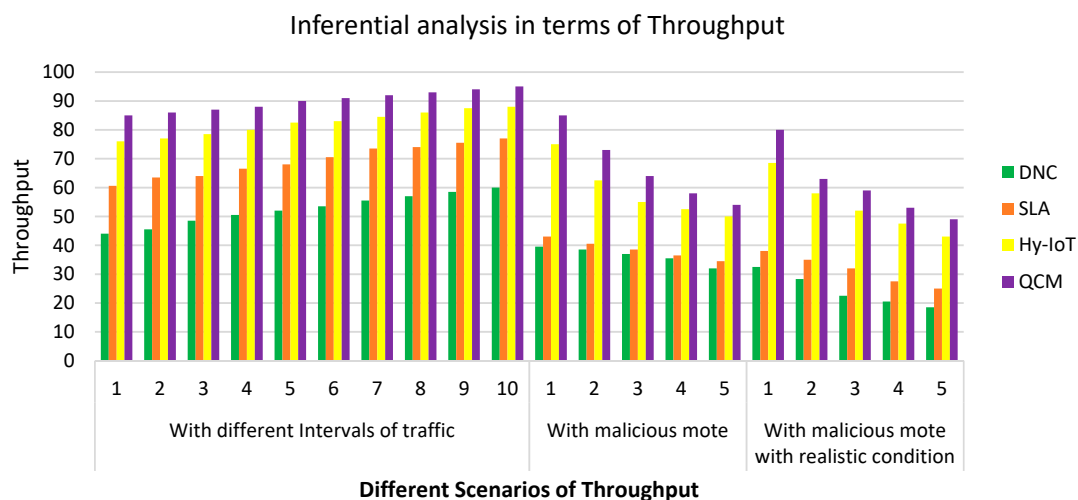
The proposed QCM is compared with DnC, SLA, and Hy-IoT using network throughput which we refer to as QoS. Here, QoS is measured for these four flooding mechanisms using three scenarios: time interval, increasing number of malicious motes and malicious motes with realistic network conditions.

Here, in this case, we discuss the performance evaluation in terms of throughput with three different scenarios, i.e., different intervals of traffic, malicious mote and malicious mote with realistic conditions.

**Table 5.** ANOVA statistics of the proposed QCM algorithm in terms of “Delay” scenarios.

“Delay” with different intervals of traffic						
Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	1454.171	3	484.7236	7.408406	0.000548	2.866266
Within Groups	2355.439	36	65.42886			
Total	3809.61	39				
“Delay” with malicious mote						
Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	673.1095	3	224.3698	4.334246	0.029825	3.238872
Within Groups	2690.596	16	168.1623			
Total	3363.706	19				
“Delay” with malicious mote with realistic conditions						
Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	2399.974	3	799.9913	3.349041	0.045503	3.238872
Within Groups	3821.948	16	238.8718			
Total	6221.922	19				

Figure 5 presents the “Throughput” with respect to different scenarios, i.e., different intervals of traffic, with malicious mote and with malicious mote and with realistic conditions. We can observe that QCM achieves the highest throughput as compared to other prevailing algorithms in the described scenarios.



**Figure 5.** Throughput with different intervals of traffic.

Table 6 presents the statistical observations of data related to the inferential analysis of QCM and other existing algorithms. We can see that the statistically significant value **P** is less than our chosen confidence interval of 0.05 which is evidence that our proposed QCM algorithm outperforms the existing algorithms. Hence, the Null hypothesis is rejected and QCM achieves the significant prediction value in the desired confidence interval.

**Table 6.** Inferential analysis of the proposed QCM algorithm in terms of “Throughput” scenarios.

<b>“Throughput” with different intervals of traffic</b>			
<i>Statistics</i>	<i>QCM and DNC</i>	<i>QCM and SLA</i>	<i>QCM and Hy-IoT</i>
Pearson Correlation	0.993765698	0.992949209	0.997823573
t Stat	59.53356302	29.60983067	28.80340889
<b>P (T ≤ t) one-tail</b>	<b>0.000000</b>	<b>0.000000</b>	<b>0.000000</b>
t Critical one-tail	1.833112933	1.833112933	1.833112933
<b>P (T ≤ t) two-tail</b>	<b>0.000000</b>	<b>0.000000</b>	<b>0.000000</b>
t Critical two-tail	2.262157163	2.262157163	2.262157163
<b>“Throughput” with malicious mote</b>			
<i>Statistics</i>	<i>QCM and DNC</i>	<i>QCM and SLA</i>	<i>QCM and Hy-IoT</i>
Pearson Correlation	0.903419023	0.986206076	0.988735878
t Stat	6.867764974	6.871919521	6.044877215
<b>P (T ≤ t) one-tail</b>	<b>0.001177169</b>	<b>0.00117451</b>	<b>0.001888935</b>
t Critical one-tail	2.131846786	2.131846786	2.131846786
<b>P (T ≤ t) two-tail</b>	<b>0.002354338</b>	<b>0.002349021</b>	<b>0.003777869</b>
t Critical two-tail	2.776445105	2.776445105	2.776445105
<b>“Throughput” with malicious mote with realistic conditions</b>			
<i>Statistics</i>	<i>QCM and DNC</i>	<i>QCM and SLA</i>	<i>QCM and Hy-IoT</i>
Pearson Correlation	0.960853622	0.938109794	0.989516045
t Stat	12.24631557	9.025002168	5.969620058
<b>P (T ≤ t) one-tail</b>	<b>0.000127655</b>	<b>0.000417442</b>	<b>0.001977709</b>
t Critical one-tail	2.131846786	2.131846786	2.131846786
<b>P (T ≤ t) two-tail</b>	<b>0.000255309</b>	<b>0.000834884</b>	<b>0.003955418</b>
t Critical two-tail	2.776445105	2.776445105	2.776445105

Table 7 presents ANOVA test statistics of the proposed QCM algorithm compared with other algorithms. We can find here that “F statistics” values are sufficiently larger than “F critical values”. In addition, the “P values” are less than 0.05, which achieves our 95% confidence interval, showing that the proposed QCM algorithm outperforms the existing algorithms evaluated through inferential analysis.

**Table 7.** ANOVA statistics of the proposed QCM algorithm in terms of “Throughput” scenarios.

<b>“Throughput” with different intervals of traffic</b>						
<i>Source of Variation</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-value</i>	<i>F crit</i>
Between Groups	1454.17075	3	484.7236	7.408406	0.000548	2.866266
Within Groups	2355.439	36	65.42886			
Total	3809.60975	39				
<b>“Throughput” with malicious mote</b>						
<i>Source of Variation</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-value</i>	<i>F crit</i>
Between Groups	673.1095	3	224.3698	4.334246	0.029825	3.238872
Within Groups	2690.596	16	168.1623			
Total	3363.7055	19				
<b>“Throughput” with malicious mote with realistic conditions</b>						
<i>Source of Variation</i>	<i>SS</i>	<i>df</i>	<i>MS</i>	<i>F</i>	<i>P-value</i>	<i>F crit</i>
Between Groups	2399.974	3	799.9913	3.349041	0.045503	3.238872
Within Groups	3821.948	16	238.8718			
Total	6221.922	19				

## 6. Discussion (Hypothesis Testing)

This research was based on the hypothesis that the proposed **QCM (Query Control Mechanism)** algorithm (Khan, F. A., Noor, R. M., Mat Kiah, M. L., Noor, N. M., Altowajri, S. M., & Rahman, A. U., 2019) outperforms the other existing algorithms, i.e., DnC, SLA, and Hy-IoT for QoS-enabled layered-based clustering for reactive flooding in the Internet of Things. The study elaborated numerous defensive techniques against unwanted and redundant routing queries which lead to heavy network traffic and flooding in IoT networks. In this study, the authors implemented the reactive part Interlayer clustering (IELC) of Cluster based flooding (CBF) and proposed a Query control mechanism (QCM) to detect and terminate the unwanted and redundant queries based on link signal strength, consistency of query packet and query limit threshold.

It is evident from the results that the proposed QCM had superior performance compared with the state of the art defensive techniques in terms of the average consumption of energy, traffic delay, and QoS which we referred to as network throughput. Thus, QCM drops the average consumption of energy to a significant rate as compared to the DnC, SLA, and Hy-IoT under varying intervals of traffic. The performance of QCM is also better regarding average consumption of energy with malicious motes against the traditional approaches by dropping the consumption at different motes. Additionally, QCM also exhibits dominant performance regarding network delay by decreasing the delay as compared to the state of the art.

In the case of malicious motes, the proposed QCM drops the network delay to a significant level. Lastly, QCM enhances the amount of QoS to a greater extent as compared to Hy-IoT. The Proposed QCM technique employs the Query Limit Threshold (QLT) for detecting and terminating the redundant and unwanted query request packets, and in this way boosts the IoT network performance in terms of signal strength of query packets and improves the location consistency checking of connected motes to keep the network away from reactive flooding attacks.

This performance clearly shows the difference between our approach and the contemporary approaches. We plan to extend this work in the future by considering a discrete component circuit implementation model using Bouali's system to detect some other attacks in IoT by extending the number and types of motes in order to test the reliability of our approach in the presence of many motes. Also, we plan to include the proactive part Intralayer clustering (IALC) of the CBF, which is favorable in high priority and less delay IoT networks, i.e., smart transportation, smart health, and smart security, and to model a physical prototype for it.

The statistical tests calculated the probability value, "P-value", based on the data sets of results for different comparable algorithms. We kept the standard confidence interval as 0.05 to determine the 95% confidence interval. "P-values" less than 0.05 were considered statistically significant. On the contrary, "P-values" larger than the chosen confidence interval inferred that the performance of comparable algorithms had no statistical significance for results and hence no algorithm outperformed the other algorithms in this comparison.

This research employed statistical measures to evaluate the performance of different QoS-enabled layered-based clustering algorithms for reactive flooding in the Internet of Things with the following measures. The inferential analysis was performed in the context of **Energy Consumption** (with different intervals of traffic, with malicious mote and with malicious mote with realistic conditions). Similarly, Inferential analysis was performed in terms of **Delay** (with different intervals of traffic, with malicious mote and with malicious mote with realistic conditions). Further, the research estimated the inferential measures in the context of **Throughput** (with different intervals of traffic, with malicious mote and with malicious mote with realistic conditions).

Based on our hypothesis theories stated earlier, we found the probability value "P" (in all statistical evaluations) remained less than 0.05, which rejected the Null hypothesis that there was no statistical significance of results for the **proposed QCM algorithm** as compared to the results of other existing algorithms, i.e., DnC, SLA, and Hy-IoT for QoS-enabled layered-based clustering for reactive flooding in the Internet of Things. Further, in the context of the alternative hypothesis, the evaluation of

performance measures revealed that the alternative hypothesis was accepted since the **proposed QCM algorithm** outperformed the other existing algorithms.

## 7. Conclusions

This research article presented a statistical performance evaluation of different query control mechanisms. The performances of such query control mechanisms rely on minimizing the energy consumption, cost and network flooding. This article simulated and evaluated the performance measure of different query control mechanisms for QoS-enabled layered-based clustering for reactive flooding in the Internet of Things. By statistical means, we infer the significant achievement of the QCM algorithm (Khan, F. A., Noor, R. M., Mat Kiah, M. L., Noor, N. M., Altowajri, S. M., & Rahman, A. U., 2019) that outperformed the prevailing algorithms, i.e., DnC, SLA, and Hy-IoT for identification and elimination of redundant flooding queries. The inferential analysis for performance evaluation of algorithms was measured in terms of energy consumption with energy consumption, delay and throughput with different intervals of traffic, malicious mote and malicious mote with realistic conditions. It is evident from the results that the QCM algorithm outperforms the existing algorithms, depicting the statistical probability value “ $P$ ” < 0.05, indicating the performance of QCM significantly achieved the 95% confidence interval. Hence, the performance of the QCM algorithm is significant as compared to the performance of other algorithms.

**Author Contributions:** Conceptualization, F.A.K. and R.M.N.; methodology, F.A.K. and R.M.N.; software, M.L.M.K., M.Y.I.I. and I.A.; validation, M.A., M.Y.I.I. and I.A.; formal analysis, M.A and F.A.K.; investigation, T.K.S. and I.A.; resources, M.L.M.K.; data correction, F.A.K.; writing—original draft preparation, F.A.K. and R.M.N.; writing—M.A. and M.L.M.K.; supervision, R.M.N and M.L.M.K.; project administration, R.M.N.; funding acquisition, R.M.N. All authors have read and agreed to the published version of the manuscript.

**Funding:** This project is funded by the Malaysia Research University Network (MRUN) Long Term Research Grant Scheme (LRGS) (LR003-2019 and LRGS MRUN/F2/01/2019/001).

**Conflicts of Interest:** The authors have no conflicts of interests.

## References

1. Abdalzaher, M.S.; Seddik, K.; Elsabrouty, M.; Muta, O.; Furukawa, H.; Abdel-Rahman, A. Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors* **2016**, *16*, 1003. [CrossRef]
2. Abdelaal, M.; Theel, O.; Kuka, C.; Zhang, P.; Gao, Y.; Bashlovkina, V.; Fränze, M. Improving Energy Efficiency in QoS-Constrained Wireless Sensor Networks. *Int. J. Distributed Sens. Netw.* **2016**, *12*, 1576038. [CrossRef]
3. End-to-End QoS Specification and Monitoring in the Internet of Things. Available online: <https://pdfs.semanticscholar.org/6156/3ae040aef11fd7dded6d39d92516c0368423.pdf> (accessed on 8 November 2019).
4. Arkian, H.R.; Atani, R.E.; Pourkhalili, A.; Kamali, S. A stable clustering scheme based on adaptive multiple metric in vehicular Ad-hoc Networks. *J. Inf. Sci. Eng.* **2015**, *31*, 361–386. [CrossRef]
5. Asif, M.; Khan, S.; Ahmad, R.; Sohail, M.; Singh, D. Quality of service of routing protocols in wireless sensor networks: A review. *IEEE Access* **2017**, *5*, 1846–1871. [CrossRef]
6. Attwood, A.; Abuelmatti, O.; Fergus, P. M2M rendezvous redundancy for the internet of things. In Proceedings of the 6th International Conference on Developments in ESystems Engineering, Abu Dhabi, UAE, 16–18 December 2013; pp. 46–50. [CrossRef]
7. Awan, I.; Younas, M.; Naveed, W. Modelling QoS in IoT applications. In Proceedings of the 2014 International Conference on Network-Based Information Systems, Salerno, Italy, 10–12 September 2014; p. 99105. [CrossRef]
8. Babar, S.; Stango, A.; Prasad, N.; Sen, J.; Prasad, R. Proposed embedded security framework for Internet of Things (IoT). In Proceedings of the 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology, Wireless VITAE, Chennai, India, 28 February–3 March 2011; pp. 1–5. [CrossRef]

9. David, D.R.; Nait-Sidi-moh, A.; Durand, D.; Fortin, J. Using Internet of Things technologies for a collaborative supply chain: Application to tracking of pallets and containers. *Procedia Comput. Sci.* **2015**, *56*, 550–557. [[CrossRef](#)]
10. Dhumane, A.; Prasad, R.; Prasad, J. Routing Issues in Internet of Things: A Survey. In Proceedings of the International MultiConference of Engineers and Computer Scientists (IMECS), Hong Kong, China, 16–18 March 2016.
11. Dlodlo, N.; Kalezhi, J. The internet of things in agriculture for sustainable rural development. In Proceedings of the 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 17–20 May 2015; pp. 13–18. [[CrossRef](#)]
12. Ebrahimi, M.; Shafiei-Bavani, E.; Wong, R.K.; Fong, S.; Fiaidhi, J. An adaptive meta-heuristic search for the internet of things. *Future Gener. Comput. Syst.* **2017**, *76*, 486–494. [[CrossRef](#)]
13. Fadele, A.A.; Othman, M.; Abaker, I.; Hashem, T.; Yaqoob, I.; Imran, M.; Shoaib, M. A novel countermeasure technique for reactive jamming attack in internet of things. *Multimed. Tools Appl.* **2019**, *78*, 29899–29920. [[CrossRef](#)]
14. Fadele, A.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of things Security: A Survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [[CrossRef](#)]
15. Gupta, A.; Christie, R.; Manjula, P.R. Scalability in Internet of Things: Features, Techniques and Research Challenges. *Int. J. Comput. Intell. Res.* **2017**, *13*, 1617–1627.
16. Gupta, H.; Vahid Dastjerdi, A.; Ghosh, S.K.; Buyya, R. iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. *Softw. Pr. Exp.* **2017**, *47*, 1275–1296. [[CrossRef](#)]
17. Haddad, H.; Bouyahia, Z.; Jabeur, N. Towards a Three-Level Framework for IoT Redundancy Control through an Explicit Spatio-Temporal Data Model. *Procedia Comput. Sci.* **2017**, *109*, 664–671. [[CrossRef](#)]
18. Huang, J.; Duan, Q.; Zhao, Y.; Zheng, Z.; Wang, W. Multicast Routing for Multimedia Communications in the Internet of Things. *IEEE Internet Things J.* **2017**, *4*, 215–224. [[CrossRef](#)]
19. Jin, J.; Gubbi, J.; Luo, T.; Palaniswami, M. Network architecture and QoS issues in the internet of things for a smart city. In Proceedings of the 2012 International Symposium on Communications and Information Technologies (ISCIT), Gold Coast, QLD, Australia, 2–5 October 2012; pp. 956–961. [[CrossRef](#)]
20. Kharkongor, C.; Chithralekha, T.; Varghese, R. A SDN Controller with Energy Efficient Routing in the Internet of Things (IoT). *Procedia Comput. Sci.* **2016**, *89*, 218–227. [[CrossRef](#)]
21. Krishnapriya, S.; Joby, P.P. QoS Aware Resource Scheduling in Internet of Things-Cloud Environment. *Int. J. Sci. Eng.* **2015**, *6*, 294–297.
22. Laxmi, P.; Deepthi, G.L. Smart Water Management Process Architecture with IoT Based Reference. *Int. J. Comput. Sci. Mob. Comput.* **2017**, *6*, 271–276.
23. Li, L.; Li, S.; Zhao, S. QoS—Aware Scheduling of Services-Oriented Internet of Things. *IEEE Trans. Ind. Inf.* **2014**, *10*, 1497–1505. [[CrossRef](#)]
24. Li, S.; Tryfonas, T.; Li, H. The Internet of Things: A security point of view. *Internet Res.* **2016**, *26*, 337–359. [[CrossRef](#)]
25. Liang, O.; Ahmet Şekercioğlu, Y.; Mani, N. A low-cost flooding algorithm for wireless sensor networks. In Proceedings of the IEEE Wireless Communications and Networking Conference, Kowloon, China, 11–15 March 2007; pp. 3498–3503. [[CrossRef](#)]
26. Vellanki, M.; Kandukuri, S.P.R.; Razaque, A. Node Level Energy Efficiency Protocol for Internet of Things. *J. Comput. Sci.* **2015**, *3*, 1–5. [[CrossRef](#)]
27. Nef, M.; Perlepes, L.; Stamoulis, G.I.G.; Karagiorgou, S.; Stamoulis, G.I.G.; Kikiras, P. Enabling QoS in the Internet of Things. In Proceedings of the CTRQ 2012: The Fifth International Conference on Communication Theory, Reliability, and Quality of Service, Mont Blanc, France, 4 May 2012; pp. 33–38. [[CrossRef](#)]
28. Nukala, R.; Panduru, K.; Shields, A.; Riordan, D.; Doody, P.; Walsh, J. Internet of Things: A review from “Farm to Fork”. In Proceedings of the 2016 27th Irish Signals and Systems Conference (ISSC 2016), Londonderry, UK, 21–22 June 2016. [[CrossRef](#)]
29. Polyvyanyy, A.; Ouyang, C.; Barros, A.; van der Aalst, W.M.P. Process querying: Enabling business intelligence through query-based process analytics. *Decis. Support. Syst.* **2017**, *100*, 41–56. [[CrossRef](#)]
30. Raju, I.; Parwekar, P. Detection of sinkhole attack in wireless sensor network. *Adv. Intell. Syst. Comput.* **2013**, *381*, 629–636. [[CrossRef](#)]



31. Rizal, R.; Riadi, I.; Prayudi, Y. Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. *Int. J. Cyber-S Secur. Digit. Forensics (IJCSDF)* **2018**, *7*, 382–390.
32. Sadek, R.A. Hybrid energy aware clustered protocol for IoT heterogeneous network. *Future Comput. Inform. J.* **2018**, *3*, 166–177. [[CrossRef](#)]
33. Yan-E, D. Design of intelligent agriculture management information system based on IoT. In Proceedings of the 2011 Fourth International Conference on Intelligent Computation Technology and Automation, Shenzhen, China, 28–29 March 2011; pp. 1045–1049. [[CrossRef](#)]
34. Khan, F.A.; Noor, R.M.; Mat Kiah, M.L.; Noor, N.M.; Altowaijri, S.M.; Rahman, A.U. QoS-enabled Layered-based Clustering for Reactive Flooding in the Internet of Things. *Symmetry* **2019**, *11*, 634. [[CrossRef](#)]
35. Ahmad, M.; Jung, L.T.; Bhuiyan, A.A. From DNA to protein: Why genetic code context of nucleotides for DNA signal processing? A review. *Biomed. Signal Process. Control* **2017**, *34*, 44–63.
36. Ahmad, M.; Jung, L.T.; Bhuiyan, A.A. A biological inspired fuzzy adaptive window median filter (FAWMF) for enhancing DNA signal processing. *Comput. Methods Programs Biomed.* **2017**, *149*, 11–17. [[CrossRef](#)] [[PubMed](#)]
37. Ahmad, M.; Jung, L.T.; Bhuiyan, A.A. On fuzzy semantic similarity measure for DNA coding. *Comput. Biol. Med.* **2016**, *69*, 144–151. [[CrossRef](#)]



© 2020 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/>).