mathematics

MDPI

Article

Development of a Model for Spoofing Attacks in Internet of Things

Faheem Khan [1,*], Abdullah A. Al-Atawi [2], Abdullah Alomari [3], Amjad Alsirhani [4,5], Mohammed Mujib Alshahrani [6], Jawad Khan [7] and Youngmoon Lee [7,*]

1 Department of Computer Engineering, Gachon University, Seongnam 13120, Korea
2 Department of Computer Science, Applied College, University of Tabuk, Tabuk 47512, Saudi Arabia
3 Department of Computer Science, Al-Baha University, Albaha 65799, Saudi Arabia
4 College of Computer and Information Sciences, Jouf University, Sakaka 72388, Saudi Arabia
5 Faculty of Computer Science, Dalhousie University, Halifax, NS B3H 4R2, Canada
6 College of Computing and Information Technology, University of Bisha, Bisha 61361, Saudi Arabia
7 Department of Robotics, Hanyang University, Ansan 15588, Korea
* Correspondence: faheem@gachon.ac.kr (F.K.); youngmoonlee@hanyang.ac.kr (Y.L.)

Abstract: Internet of Things (IoT) allows the integration of the physical world with network devices for proper privacy and security in a healthcare system. IoT in a healthcare system is vulnerable to spoofing attacks that can easily represent themselves as a legal entity of the network. It is a passive attack and can access the Medium Access Control address of some valid users in the network to continue malicious activities. In this paper, an algorithm is proposed for detecting spoofing attacks in IoT using Received Signal Strength (RSS) and Number of Connected Neighbors (NCN). Firstly, the spoofing attack is detected, located and eliminated through Received Signal Strength (RSS) in an inter-cluster network. However, the RSS is not useful against intra-cluster spoofing attacks and therefore the NCN is introduced to detect, identify and eliminate the intra-cluster spoofing attack. The proposed model is implemented in Network Simulator 2 (NS-2) to compare the performance of the proposed algorithm in the presence and absence of spoofing attacks. The result is that the proposed model increases the detection and prevention of spoofing.

Keywords: spoofing attack; IoT; RSS; NCN; healthcare system; NS-2 simulator

MSC: 68U01

Citation: Khan, F.; Al-Atawi, A.A.; Alomari, A.; Alsirhani, A.; Alshahrani, M.M.; Khan, J.; Lee, Y. Development of a Model for Spoofing Attacks in Internet of Things. *Mathematics* **2022**, *10*, 3686. https://doi.org/10.3390/math10193686

Academic Editor: Ximeng Liu

Received: 21 August 2022
Accepted: 24 September 2022
Published: 8 October 2022

1. Introduction

The privacy of IoT devices is vulnerable to security attacks as compared to wired network due to the shared wireless medium. In addition, due to limited resources in terms of battery capacity and computation, lightweight protocols are preferred, and such protocols are vulnerable to all kinds of security attacks [1]. There are three major areas in which the IoT could be compromised maliciously, i.e., through physical access, unauthorized access to local network and remote access through internet. Furthermore, there are two types of attacks, i.e., internal attacks and external attacks. Internal attacks are more severe as compared to external attacks and it is critical to develop such protocols that can detect and identify the attackers within the IoT [2]. Some of the challenges of spoofing attacks are communication of false information within the IoT system, vulnerability of IoT devices, compromising the decision-making process, manipulation of the operation of the IoT system [3], repeated routing loops [4,5] passive listening of the communication and showing itself as a legitimate device within the IoT pool of devices to operate malicious activities [6], and severeness of spoofing attack on time-dependent IoT devices such as robotic arms in the industry [7].

Spoofing attacks compromise both wired and wireless networks maliciously. The malicious entity accesses the device, resources and network by using the frames and fields with address identifiers of the target user, and these addresses can be the MAC address or IP address [8]. There are many kinds of spoofing attacks such as email, URL and frame spoofing attacks, but the common attacks are either MAC address or IP address spoofing attacks [9]. MAC address is used on data link layer and considered as an authentication factor for wireless networks in IoT. In a spoofing attack, the malicious entity modifies the MAC address to some forged value that belongs to the valid user and obtains illegal benefits in the network [10]. To detect spoofing attacks, physical layer authentication is used through RSS.

Many authentication techniques detect spoofing attacks on a wireless medium through RSS [11,12], channel frequency response [13] and channel state information [14]. This method [15] describe spoofing attack in a wireless channel across the network reference point and present an explanation of spoofing attack in vehicular network. This paper [16] discussed the process of elimination through wireless traffic by classifying the MAC sequence number of the incoming packet.

Contribution of the Paper

In a health care system, if the information of the patient is compromised maliciously then it is an alarming situation and the patient can be in danger. Similarly, modifying the information of security cameras, smart homes, smart automobiles, smart industries and many other IoT-related devices could lead to a disaster. In IoT, a kind of algorithm that detects, identifies and eliminates spoofing attacks in both inter-cluster and intra-cluster network is lacking. In this paper an algorithm is designed that will detect, locate and eliminate the inter-cluster and intra-cluster spoofing attacks by using the following contribution.

- To detect, locate and eliminate the spoofing attack through Received Signal Strength (RSS) within the inter-cluster wireless network.
- To detect, identify and eliminate the spoofing attack through the Number of Connected Neighbors (NCN) within the intra-cluster wireless network.

In this paper, NS-2 simulator is used to determine the spoofing attack. For RSS, parameters of delay and negative ack are used to detect spoofing attacks. In the presence of a spoofing attack, the delay and negative ack increases, which affects the performance of the IoT devices. This increase in delay and negative ack is very crucial in healthcare systems and the patient's life can be threatened. For NCN, parameters of delay and energy are used to detect spoofing attacks. In the presence of spoofing attacks during NCN, when the delay increases then the energy consumption also increases. This increase in energy consumption increases the battery consumption of the IoT devices and in turn decreases the lifetime of the cluster. Hence, the wireless connected nodes will be disconnected from the cluster and the patient's life can be in danger.

With the help of these techniques, the spoofing attack is detected, identified and eliminated. The organization of the paper is as follows. In Section 2, the literature work is discussed relevant to spoofing attacks in IoT networks with the security of the wireless network. Section 3 describes the proposed methodology of an inter-cluster and intra-cluster method along with a proposed model of the paper. Section 4 is explaining the comparison of the results for RSS and NCN in the presence and absence of spoofing attacks separately. Finally, Section 5 describes the conclusion of the paper.

2. Related Work

In this paper [17], a detection of spoofing attacks is discussed based on spatial correlation of the RSS in wireless network. A k-means algorithm computes a comparison metric for the detection of attack. A propagation model for spatial correlation of RSS is included for the path loss and shadowing effects and it did not consider a fast shadowing effect. As a result, a fading effect the detection process of instant RSS samples. Similarly, the detection

process does not perform and the protocol fails when the actual node and the spoofing entity are close to each other.

The objective of this paper [18] is to detect and mitigate network-based spoofing attacks. This paper first shows the detecting of DDoS attacks in the compromised IoT devices through WiFi network. This paper then demonstrates that by mitigating the attack, the resource consumption of IoT devices decreased within the network.

The increased use of geo-spatial location-based application for IoT location-based spoofing attacks [19]. A Secure Location of Things (SLOT) framework is developed to overcome the attack and provide information about whether the source node successfully communicated with the destination node or not. This information will reformulate the location estimation problem and provide the maximum likelihood of the node location.

In this paper, virtual spoofing attack is detected through channel state information (CSI). The proposed Virtual MAC Spoofing detector (VMASC) extracts the features of amplitude and phase from the CSI to classify devices and improve the detection accuracy [20].

This paper [21] describes the identity of spoofing attacks on IoT devices. This attack is on the 5G communication and is very difficult to detect due to its wireless nature. In this paper a two-step detection scheme is proposed by connecting virtual channels with mm-Wave and Massive MIMO 5D. In the first step, an attack is detected by investigating the Angle of Arrival (AoA) and path gains of IoT devices in a virtual channel space. In the second stage, a machine learning detection technique is introduced. Simulation results show the improvement of Bayes risk in the presence of IoT devices.

This method [22] used channel state information (CSI) to detect MAC spoofing attack, which depends on Profile Matching Authenticator (ProMA). It uses the amplitude data of CSI to make a specific pattern of profile for each legal device in the network. As a result, it is simple to detect spoofing attacks by the unusual pattern of each device. This unusual pattern shows the amplitude information from different devices at different locations and the spoofing device can be detected having different profile construction. The drawback of this approach that all the profiles should be updated regularly, which increases the overhead and hence may not be useful in many situations.

The above-mentioned approaches are using matching rules for the detection of spoofing. These approaches have different detection and false alarm rates but none of the methods provide detection, localization, identification and elimination of the spoofing attack for both inter-cluster and intra-cluster IoT-based network. The proposed protocol detects, identifies, localizes and removes spoofing attacks for inter-cluster and intra-cluster IoT-based networks, as shown in Table 1.

Table 1. Comparison of Protocols.

Protocol/ Algorithm	Research Problem	Objectives	Contributions	Domain	Simulator	Evaluation Metrics	Limitation of Study
[17]	Identity based spoofing attack	Detection	Improvement of fast fading effects, spatial and time correlations	RSS	MATLAB	Distance, time and location, power	Only detection
[18]	DDoS based spoofing attack	Detection and mitigation	Saving power consumption	Traffic monitoring through DHCP	Not mentioned	Throughput and number of exchange flow	Only Detection and mitigation

Table 1. *Cont.*

Protocol/ Algorithm	Research Problem	Objectives	Contributions	Domain	Simulator	Evaluation Metrics	Limitation of Study
[19]	Information altering and signaling attack	Localization	Improvement in location identification	Location estimation technique	Monte Carlo	Transmission power and distance	Only Localization
[20]	Identity based spoofing attack	Detection	Improvement of accuracy	CSI	Real time experiment	Amplitude and Phase of channel	Only detection
[21]	Identity based spoofing attack	Detection	Improvement of Bayes risk	mm-Wave and massive MIMO virtual channel	Not mentioned	SNRs and number of antennas	Detection
[22]	MAC spoofing attack	Detection	Improvement of accuracy	CSI	Real time experiment	Amplitude and Phase of channel	Only detection
Proposed method	Identity based spoofing attack	Detection, identification and removal	Improvement of Energy consumption, delay and Negative ACK (accuracy)	RSS and NCN	NS-2 Simulator	Energy, delay and Negative ACK	Absence of comparison and will do in future work

3. Methodology

This paper presents a model that detects, localizes, identifies and eliminates the spoofing attack within the cluster as shown in Figure 1.

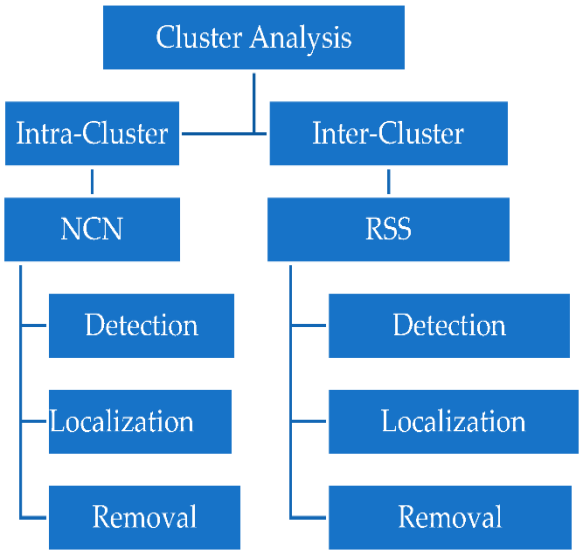

Figure 1. Detection, localization, identification and removal of spoofing attack.

In this paper, the IoT network [23–26] is divided into clusters for the detection and localization of the spoofing attack accurately because there are limited nodes in the cluster. The cluster forms a group of nodes with similar interests and the cluster is maintained by the core node through a Status Declaration (SD) message or Hello message. SD messages

inform about the status of each node in the group or about the entry of new nodes and exit of the existing member node.

The clusters are monitored through detection and localization method to identify and remove the spoofing attack. The cluster is further divided into intra-cluster and inter-cluster. In the former approach, the communication between the two or more clusters is possible and in the later approach the communication within the cluster is used. RSS and NCN techniques are suggested for the detection of spoofing attacks. RSS is used for inter-cluster, where the spoofing attack is detected, localized and eliminated from the different clusters. On the other hand, NCN is used to detect, localize and eliminate the spoofing attack within the cluster, as shown in Figure 1.

3.1. Spoofing Attack Detection, Localization and Elimination through Received Signal Strength (RSS)

In this paper, the RSS-based correlation is inhibited by wireless infrastructure to execute detection using a spoofing attack from the surrounding wireless devices in a cluster-based approach. Detection of spoofing attacks is simple and accurate through RSS because cryptography is avoided. Likewise, using RSS to detect spoofing does not need any extra modification or cost in the existing wireless devices. Through RSS reading, the location and cluster of the spoofing attack could be identified by measuring the distance. In RSS, reading in term of distance are different because different nodes are operating from different locations/clusters at the same time. As shown in Figure 2, the network is divided into three clusters (K = 3) and each cluster has its core node, i.e., A, B and C. The green node shows a legitimate user and the red nodes show a spoofing attack. In a spoofing attack, the legitimate user and the attacker are sharing the mixed reading and will not be able to detect the spoofing attack. To detect the spoofing attack, cluster-based analysis is used to find the distance between the two cores and to find the physical presence of a spoofing attack in a specific cluster. It is assumed that at t_1 a core will communicate once with a node *n*. Let us suppose that core C is having a maximum radio range of 100 m and a minimum of 30 m. In normal conditions, the core will operate in a radio range of 100 m. The core node records and saves the time and distance of a valid user. At the same time, the two spoofing attacks in clusters B and A also communicate with core C within a 100-m range from different clusters. Therefore, at the same time, the core node is communicating with three different nodes and therefore the distance will increase from 100 m to 300 m because each time core C communicates with each node in the different cluster and increases the distance. Now core C receives the information from the same ID but with a larger distance and shows the presence of spoofing attacks.

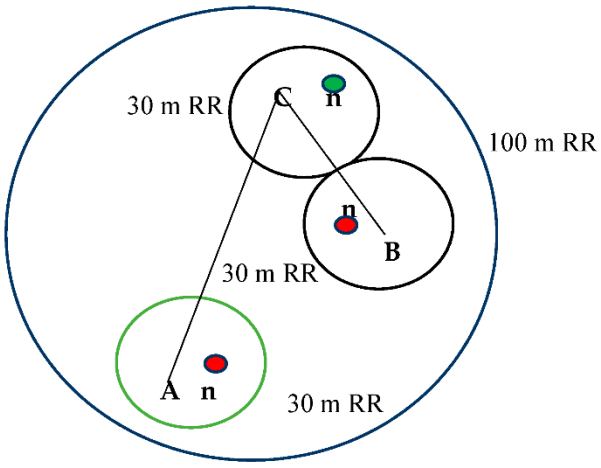

Figure 2. Spoofing Attack through Received Signal Strength (RSS).

Through RSS, the energy of the spoofing attack and legitimate node can be calculated within two or more clusters. This uses a Three Cluster model using the *K* clusters, and in

RSS the number of clusters are three, i.e., $K = 3$. Now the Three Cluster model is used for the calculation of energy, i.e., number of transmitted and received packets between the clusters. The Neighboring Energy $En(K)$ shows the distance between the nodes in the clusters and $Een(K)$ shows the Edge Energy on the edge of each cluster. The reference point in each cluster i.e., A, B and C are represented as SA, SB and SC sample points and it can be represented as $Pz = \frac{\sqrt{S_A+S_B+S_C \ldots S_n}}{3}$, where P represents the partition between the clusters and 3 represents the number of clusters. Thus, the Neighboring Energy $En(K)$ is calculated as SA and the Edge Energy $Een(K)$ is represented as Equation (2).

$$En(K) = \frac{1}{N_A+N_B+N_C}\{\sum_{i=1}^{N_A} min_{J=k=1,\ldots\ N_{B,\ldots}N_C}\ P(A_i, B_j, C_k) + \sum_{J=1}^{N_B} min_{i=k=1,\ldots N_{A,\ldots.}N_C} P(A_i, B_j, C_k) + \sum_{k=1}^{N_C} min_{i=j=1,\ldots N_{A,\ldots}N_B} P(A_i, B_j, C_k)\} \quad (1)$$

$$Een(K) = \frac{1}{N_A + N_{B+}N_C} \sum_{i=1}^{N_A+N_B+N_C} \sum_{j=(k=i)+1)}^{N_A+N_B+N_C} \sum_{k=(j=i)=1}^{N_A+N_B+N_C} P(ei,\ ej,\ ek) \quad (2)$$

where $P(A_i,\ B_j,\ C_k)$ represents the Euclidean distance between the nodes A_i, B_i and C_i in cluster A, B and C. Similarly, $P(ei,\ ej,\ ek) \in \{A_i\} \cup \{B_i\} \cup \{C_i\}$ are the nodes on the edge of the clusters between the three clusters.

Equations (1) and (2) is used to calculate the energy utilization by the node. However, if this energy is greater than the threshold value [27] then the spoofing attack is detected as shown in Equation (3) because the number of negative ACK in increasing, which ultimately is the resending of packets and hence increases the energy utilization.

$$En(K) + Een(K)\ \geq Threshold\ value \quad (3)$$

After the detection, the method of localization is started through unicasting because unicasting is not reliable within the larger distance in wireless environments. In wireless networks, there is a frequent topology change, which does not favor the unicasting. Hence, the spoofing attack within a larger distance or in another cluster could not receive the packet on its first attempt. As a result, negative acknowledgment increases to the source node. To localize the spoofing attack, the data transmission is divided into time slots. Suppose a 2-min time slot is allotted for the transmission and reception of data as shown in Table 2. At the end of the 2 min, the total delay is 1 min and 33 s and the total number of negative ACK is 4. It is clear from the table that nodes from the other clusters are acting as spoofing nodes.

Table 2. Spoofing Attack through Radio Range.

S. no	Request Time	Negative ACK	Receive Time	Delay	Number of Negative ACK
C	00:02	No	00:05	00:03	0
B	00:25	Yes	00:55	00:30	2
A	00:55	Yes	01:55	01:00	2
Total	...	...	...	1:33	4

Now, core node C will minimize its radio range within 30 m by starting the elimination process. As a result, the delay will come down to 3 s and the negative ACK reduces to zero because cluster B and A are not entertained. This information of the spoofing node is shared to core node B and A and both the cores will not entertain the request from the concerned spoofing node and will be eliminated automatically (Algorithm 1).

Algorithm 1. ***For the Detection, Identification and Removal of Spoofing attack***

Input:
TH: Threshold value (10%)
Cn: Core node
Begin:

1. *If* C_n > *TH; then*
2. $n_i \leftarrow 1$;
3. *Send unicasting;*
4. *Break*
5. *Otherwise, Continue*
6. *End if*
7. *If Neg ACK == TH && Delay == TH; then*
8. *Max RR < 1;*
9. *Delete* n_i;
10. *Go back to step 1;*
11. *End if*

End Algorithm

1. First, the core node checks whether the distance increases from the threshold value or not and it is assumed that threshold value is 100 m.
2. If it is greater than the threshold value then it shows the presence of spoofing attack. Here, 1 represents spoofing attack.
3. As soon as the spoofing attack is detected, core C sends the data through unicasting to the legitimate node as well as to the spoofing node.
4. Now if the spoofing attack is not detected then go to step 1, but if it is detected then continue towards step 3.
5. In wireless networks, unicasting is not reliable due to frequent topology changes. Therefore, a node in another cluster will receive the information but after two or three or more attempts. As a result, this increases the negative ACK and delay, having some predefined threshold value for negative ACK and delay. After exceeding the threshold value, the radio range will decrease to 30 m. The Max RR shows maximum radio range, which is 100 m, and after that the detection the radio range drops to 30 m.
6. As a result, the spoofing attack in another cluster will not be entertained and hence deleted automatically.
7. After removing the spoofing attack, the process will again start from the first step.

3.2. Spoofing Attack Detection, Localization and Elimination through Number of Connected Neighbors

Through RSS the spoofing attack in other clusters can be detected, identified and removed easily, but if the spoofing node is within the same cluster, then RSS cannot detect such spoofing attacks. Now, to detect and localize the spoofing attack within a cluster, the approach of neighbors detection technique is introduced. In a cluster-based approach, a core node is selected based on many parameters such as central position in the group [26–28], high battery capacity, low mobility, etc. The data forwarding, maintaining and updating in a cluster-based network is provided through SD message and connectivity list. The SD message is periodically (single cycle) flooded to maintain and update the group. The SD message contains the group ID, core ID and sequence number, number of connected neighbors, battery capacity, etc. Through the SD message, a connectivity list is formed. The connectivity list as shown in Figure 3 allows the data to select the best possible route to the destined node through parent node. Parent node shows the shortest path to the core node. All the group members in the cluster receive neighbor information through an SD message and store it in the connectivity list. The connectivity list is formed as follows:

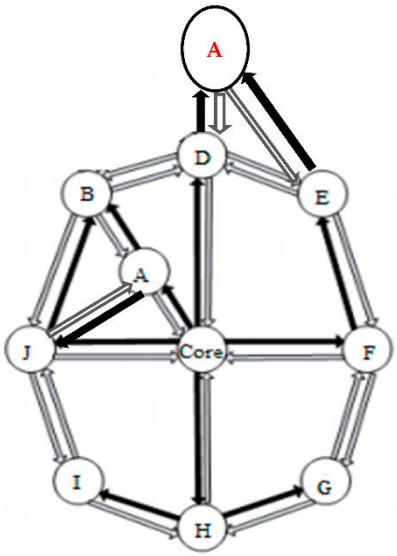

Figure 3. Connectivity list of NCN.

A group member with a fresher sequence number within a neighborhood is selected as compared to the group member having a lower sequence number. Now, a group member with less distance having the same core and fresher sequence number is preferred to store in the connectivity list. Now, a group member with high battery capacity, less distance with the same core and fresher sequence number is preferred to store in the connectivity list.

Finally, when all the fields are same, the node that received earlier will be the suitable neighbor to store in the connectivity list. Through NCN, the connected neighbors share the information of each neighbor, whether it is a legitimate node or a spoofing node, and store all the information in the connectivity list.

With the help of NCN, the energy of the spoofing attack and legitimate node can be calculated within the cluster. This uses a Single Cluster model using the K clusters, and in NCN the number of clusters are 1, i.e., $K = 1$ and it is represented as z. Now the Single-Cluster model is used for the calculation of Energy i.e., number of transmitted and received packets. The Neighboring Energy $En(K)$ shows the distance from the nearest neighbor (D and E) node and Core Energy along with Neighboring Energy $Ecn(K)$ shows the distance from the core nodes and other neighboring nodes. The reference point in a cluster z contains a total Sz sample points and it can be represented as $Pz = \frac{\sqrt{Sz}}{Nz}$, where P represents the partition and Nz represents the number of clusters and in this situation, it is 1. Thus, the Neighboring Energy $En(K)$ is calculated as

$$En(K) = \frac{1}{Nz}\{\sum_{i=1}^{N_A} min_i = 1P(z_i)\} \tag{4}$$

and the Core Energy along with Neighboring Energy $Ecn(K)$ is represented as

$$Ecn(K) = \frac{1}{Nz}\sum_{i=1}^{Nz+Nc-1}\sum_{j=i+1}^{Na+Nc} P(z_i) \tag{5}$$

where $P(z_i)$ represents the Euclidean distance between the nodes in cluster z.

$$En(K) + Ecn(K) \ \geq Threshold\ value \tag{6}$$

Equations (4) and (5) are used to calculate the energy utilization by the node. However, if this energy is greater than the threshold value then the spoofing attack is detected as shown in Equation (6).

The localization process started after the detection process. In Figure 3, node A with neighbors B, core and J are legitimate nodes. On the other hand, node A with neighbors

D and E is a spoofing attack. The SD message is periodically updating the group and the period can be defined as 3 sec or single cycle. In a single cycle, a single entry is allowed in the connectivity list with a fresher sequence number for a specific neighbor. Now, in time t1, both the legitimate and spoofing attack flood the SD message in the group members. As a result, the group receive two SD messages from the same identity, i.e., node A. At this stage the spoofing attack is identified. To localize the spoofing attack, all the neighbors are requested to share the list of the neighbors. In this situation, node B, core and J will show the presence of node A (legitimate node) and node E and D will also show the presence of node A (spoofing attack). Now, at this stage, the spoofing attack is detected as well as localized.

The neighborhood of legitimate and spoofed node A is already detected and localized. To eliminate the spoofing attack, Data Transmission and Reception (DTAR) by node is used. In DTAR, the neighborhood (Core, J, B, D and E) is requested to exchange the information related to the data transmission and data reception to both nodes. To know the amount of data received and transmitted by the neighborhood node, a Data Transmission and Reception Message (DTRM) by core node is flooded inside the group by the core node for a predefined time, i.e., 3 sec. In reply, all the members of the group flood a DTRM within the group. Thus, all the members of the cluster will know the information of each other related to data transmission, reception, Parent Node (PN) and distance to the core and store it in the connectivity list.

Spoofing attack is always greedy to receive more data and transmit less to the neighboring node. In MAC, a spoofing attack is difficult to identify between the legitimate and spoofed node and therefore through the connectivity list the information is taken from the neighboring node. It makes it easy to identify the spoofing attack from the connectivity list through neighboring node, cluster node identity, parent node, distance to the core (DC), number of transmitted packets and number of received packets. The connectivity list is explaining column wise how to identify a spoofing attack. From columns 1, 2 and 3, it is not possible to identify between legitimate node and spoofing attack however, it is assumed for proper understanding. From column 4, the parent node of legitimate node and spoofing attack is different. Similarly, the distance from the core is also different in column 5. In columns 6 and 7, there is a considerable difference between the transmitted and received packet. The transmitted packet is the packet transmission from the Neighboring Node (NN) to the node A and received packet is the packet reception from the node A, as shown in Table 3.

Table 3. Connectivity list for spoofing attack.

Legitimate or Spoofing Node	NN	CH	PN	DC	Transmitted Packet	Received Packet
Legitimate A	Core	Core node	Core node	1	10 MB	5 MB
Legitimate A	B	Core node	Core node	1	6 MB	3 MB
Legitimate A	J	Core node	Core node	1	12 MB	26 MB
Spoofing node, A	D	Core node	D	2	20 MB	2 MB
Spoofing node, A	E	Core node	D	2	30 MB	3 MB
Total					68 MB	34 MB

It is clear from the connectivity list that during the predefined period the neighbor of B, J and core is behaving normally with a normal range of packet transmission and reception. On the other hand, the neighbor of D and E is not behaving normally and there is a considerable difference between the packet transmission and packet reception. As a result, the neighboring node D and E will be informed through SD message not to entertain the request of the spoofing attack, which is a two-hops distance away from the core with a different parent node, only a legitimate node A should be entertained.

Algorithm for the Detection and Identification of Spoofing Attack

In this algorithm(Algorithm 2), the spoofing attack is detected and identified. A spoofing attack is discarded with the help of the connectivity list through core ID, distance to the core, parent node, packet transmission and reception.

To design an algorithm for the detection and removal of spoofing attack, the following conditions are required: (1) To detect the spoofing attack through SD message (2) To localize, identify and remove the spoofing attack from the cluster. In detection, a single cycle of 3 s is used for all members "Ai" of the cluster. If two requests "n Req" within a single cycle are received from the Ai then it shows the presence of the spoofing attack because it is assumed that only a single request can be used in a single cycle. Here, n represents number and Req represents requests, i.e., number of requests. In the identification and removal of the spoofing attack, many conditions of the connectivity list are calculated, such as parent node, core ID, distance to core, packet transmission and reception. The algorithm is performed on each node in the cluster by assuming that each node in the cluster will be aware of its neighborhood through the connectivity list. A threshold of 100 MB is used for transmission and reception and if it exceeds this limit then it assumed it is a spoofing attack.

To detect the spoofing message, four types of messages are used, i.e., DTAR request message by the core node to the neighboring for the amount of packet transmission and reception, DTAR reply message from the neighboring to the core node for the amount of packet transmission and reception, SD message about the identification and elimination of the spoofing attack by the core node. The algorithm has two phases; phase 1 is for detection of the spoofing attack and phase 2 is for identification and removal of the spoofing attack.

Algorithm 2. ***For the Detection and Identification of Spoofing attack***

Input:
A_i: Cluster members
DTAR: Data Transmission and Reception
Begin:

1. *If A_i == n_{Rep} then,*
2. *A_i == 1*
3. *Flood DTAR Req*
4. *Neighbor ACK == 1*
5. *Flood DTAR Rep*
6. *Break*
7. *Otherwise, Continue*
8. *End if*
9. *If DTAR $\geq$ TH then*
10. *Flood SD message*
11. *Neighbor Ack*
12. *Check Connectivity List*
13. *Delete A_i*
14. *End if*

End Algorithm

1. In detection, if at the same period two or more requests are received by the core node then it is assumed that spoofing exist in the cluster and it is represented by 1.
2. After the detection of the spoofing attack the core node floods the DTAR Req to all neighboring nodes to receive the data transmission and reception of each other.
3. The acknowledgment request of the neighbor from the core is represented from 1.
4. Now, all the members flood the requested data to the neighboring nodes and then move to step 3.
5. However, if there is no detection of the spoofing attack then go back to step 1.
6. In phase 2, the spoofing attack is identified because the data transmission is greater than the threshold value.

7. At this stage, the core node floods the SD message in the cluster members, especially to the neighbor of Ai about the presence of the spoofing node.
8. All neighbors of Ai check the connectivity list and check which node has a large difference in data transmission and reception. Similarly, the parent node is also different, with different distance from the core in term of hop distance.
9. As a result, Ai is deleted, with large data transmission, different core node and more distance from the core node.
10. When the spoofing node is removed, it will go to step 1 to detect spoofing.

4. Results Discussion and Simulation

This protocol is implemented in Network Simulator-2.35. In this simulation, Tcl/Otcl are used as a front-end language and C++ as a back-end language. AWK SCRIPT is used for data collection from trace files and BASH script is for simulation of 30 random scenario. The following parameters are used as shown in Table 4.

Table 4. Simulation Parameters.

Simulator	Network Simulator (NS2)
Examined Attack	Spoofing Attack
Number of nodes	40
Transmission range	30–100 m
Simulation area	1000 m × 1000 m
Simulation time	450 sec
Data packet size	512 bytes
MAC type	MAC 802.11
ifqLen	60
Size of routing queue	50 packets
Total number of generated packets	10,000

The following metrics, i.e., delay, negative acknowledgment and energy. Delay is defined as the round-trip time between receiver node and sender node and negative ACK alerts the sender that the message is not yet received. This paper defines the negative acknowledgment in term of numbers, i.e., number of negative ACK received by the sender, and will explain the result of NCN and RSS.

4.1. Matrices

The following matrices are used to calculate the parameters as shown in Table 3.

Delay is the time taken by the data packet on transmission link.
Delay = Size of data Packet/Bandwidth of Network [29].
Energy shows difference between current energy and initial energy. Here initial energy represents starting of experiment [30].
Energy = Initial Energy—Current Energy
Negative ACK represents the damaged or duplicate packet received by the receiver. The receiver sends a negative ACK back to the sender and the sender retransmits the packet.

4.2. Results of RSS

In this section, two scenarios evaluate the network performance in the presence of a spoofing attack.

Scenario 1: In the presence of a spoofing attack using a radio range of 100 m.
Scenario 2: In the presence of a spoofing attack using a radio range of 30 m.

In scenario 1, the proposed method is used for the detection of a spoofing attack. As shown in Figure 2, there are three clusters and two core nodes, i.e., B and C having a spoofing attack. When the spoofing attack increases, there will be an increase in the distance for the same ID as discussed earlier. At this situation, unicasting detects and identifies the

spoofing attacks. As soon as the unicasting starts, negative ACK increases. This increase in negative ACK is due to the increase in distance between the two clusters as shown in Figure 4. The data is dropped due to unicasting and mobility. In normal situations, broadcasting is used, but for the detection of a spoofing attack, unicasting is used, which is the unreliable approach in wireless networks, wireless sensor network (WSN) [31–33] and mobile ad-hoc networks.

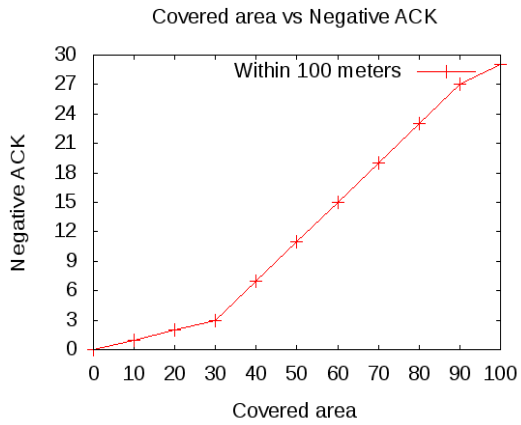

Figure 4. Negative ACK due to presence of spoofing attack.

As shown in Figure 4, when the distance is increasing, the number of negative ACK also increases, which shows the presence of the spoofing attack outside the cluster. This increase in negative ACK increases the trafficking, congestion and energy consumption. As a result, the lifetime of the node and lifetime of the core of the concerned cluster also decrease.

The core failure will start the reconfiguration between the group member for another core and increases the overhead. This reconfiguration and packet drop will also increase the delay. As shown in Figure 5, by increasing the distance up to 100 m and with the increase in negative ACK, this increases the delay. As a result of the spoofing attack, the resources of the group are consumed quickly and the communication cannot be considered reliable.

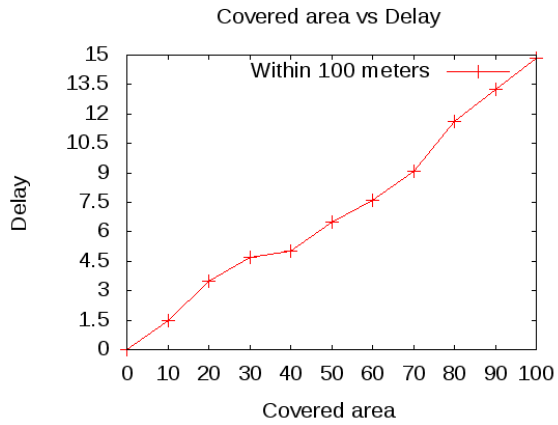

Figure 5. Delay due to presence of spoofing attack.

Now, scenario 2 is used after the detection and identification of the spoofing attack, where the radio range of each cluster is up to 30 m. As a result, spoofing nodes in the other clusters are not entertained and only the node within the clusters is entertained from the communication. This decreases the negative ACK because nodes within the cluster are with less distance and hence packet drop decreases and a successful communication is increasing between the source and the destination. As shown in Figure 6, only one negative ACK appeared, which is normal within a mobile environment.

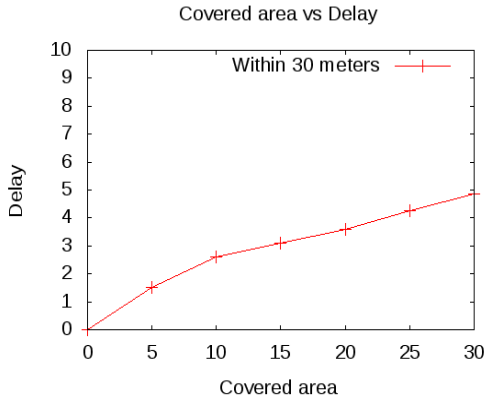

Figure 6. Negative ACK due to absence of spoofing attack.

As the negative ACK decreases, there is a decrease in the packet drop and core reconfiguration, which ultimately decreases the delay as shown in Figure 7. Hence, the node in the group behaves normally in terms of negative ACK and delay.

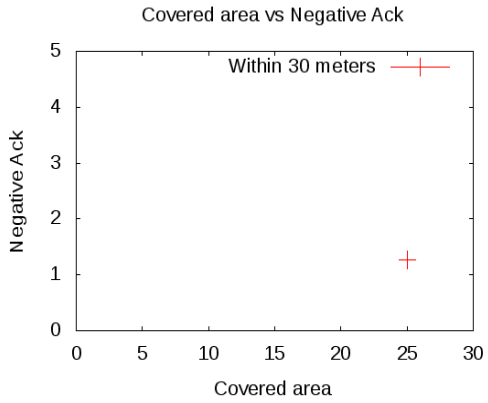

Figure 7. Delay due to absence of spoofing attack.

4.3. Results of NCN

In this section, two scenarios evaluate the network performance in the presence and absence of a spoofing attack. Figure 8 shows the simulation under the normal conditions, i.e., in the absence of a spoofing attack. It shows that the energy is consumed in a normal rate and hence the lifetime of the cluster increases. The Figure 8 shows that in the presence of five legitimate nodes, 46 joules of the energy are consumed. On the other hand, in the presence of a spoofing attack, 80 joules of energy are consumed, and with the increase in spoofing attack the energy consumption increases, as shown in Figure 9.

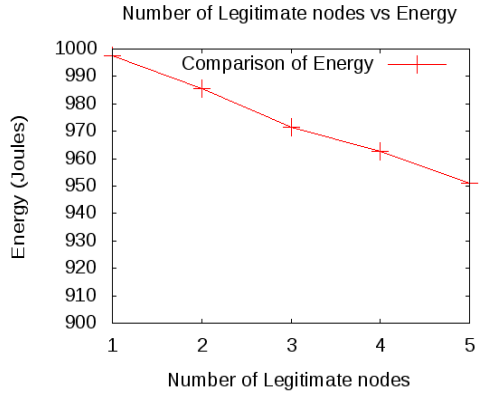

Figure 8. Energy in the absence of spoofing attack.

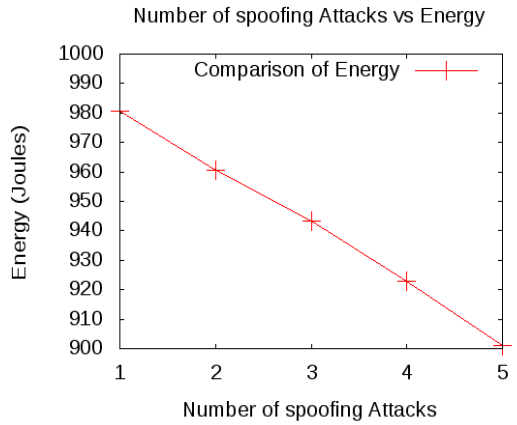

Figure 9. Energy in the presence of spoofing attack.

Figures 10 and 11 show the presence and absence of a spoofing attack in terms of delay. Hence, in the presence of a spoofing attack, there is an unbiased distribution of data between the legal node and the illegal node and hence the desired node is not receiving the data because the illegal node consistently requests the data. Hence, this increases the congestion and traffic in the cluster, which ultimately increases the delay as compared to normal conditions when there is no attack.

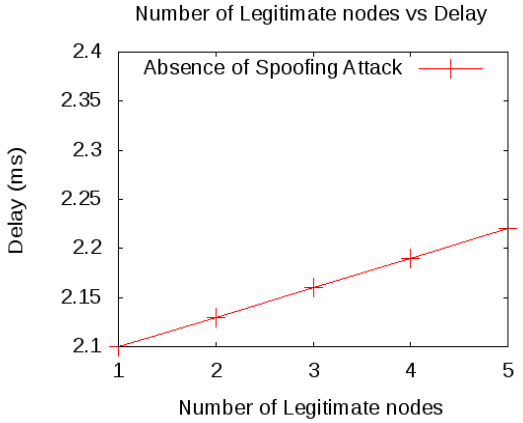

Figure 10. Delay in the absence of spoofing attack.

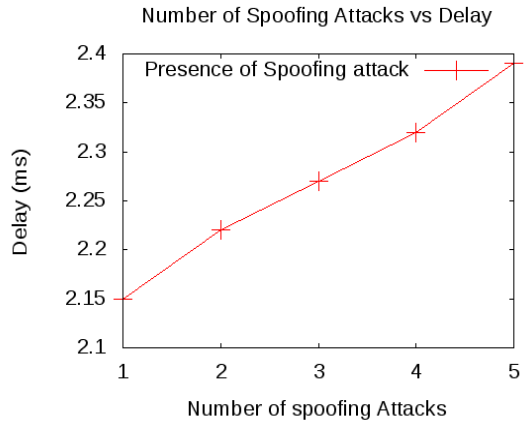

Figure 11. Delay in the presence of spoofing attack.

5. Conclusions

In this paper, a spoofing attack is discussed in an inter-cluster-based network and an intra-cluster-based network. The spoofing attack is detected through RSS and NCN in inter-cluster approach and intra-cluster approach for detection, localization and elimination. The results show that using unicasting in an inter-cluster network increases the packet drop and will increase the negative ACK. As a result, this increases the delay and will detect the spoofing attack within the specific cluster through an increase in the negative ACK and delay.

The detection of spoofing attacks through RSS is useful for inter-cluster communication, but for intra-cluster spoofing attacks, the NCN approach is useful. The spoofing attack is detected through NCN in the intra-cluster approach through energy parameters. The results show that the compromised node consumed more energy as compared to the non-compromised node. Similarly, due to malicious behavior, the transmission of illegal communication also increases, which increases the congestion and hence increases the delay. Finally, for elimination processes in the NCN of spoofing attack, DTAR is used. The results show that in the presence of RSS and NCN, the spoofing attacks are very limited and the performance of the network is improved. However, in the absence of spoofing attack the performance of the network is decreasing continuously.

Author Contributions: Conceptualization, F.K.; Formal analysis, M.M.A. and J.K.; Funding acquisition, Y.L.; Investigation, A.A. (Abdullah Alomari), A.A. (Amjad Alsirhani), J.K. and Y.L.; Methodology, F.K.; Project administration, A.A.A.-A. and M.M.A.; Resources, A.A. (Abdullah Alomari), A.A. (Amjad Alsirhani), J.K. and Y.L.; Software, A.A.A.-A.; Validation, F.K., A.A.A.-A., A.A. (Abdullah Alomari), J.K. and Y.L.; Writing—original draft, F.K.; Writing—review & editing, A.A.A.-A., A.A. (Abdullah Alomari), A.A. (Amjad Alsirhani), M.M.A., J.K. and Y.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the research fund of Hanyang University (HY-2022-2561).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Li, Q.; Trappe, W. Light-weight detection of spoofing attacks in wireless networks. In Proceedings of the 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems, Vancouver, BC, Canada, 9–12 October 2006; pp. 845–851.
2. Jindal, K.; Dalal, S.; Sharma, K.K. Analyzing spoofing attacks in wireless networks. In Proceedings of the 2014 Fourth International Conference on Advanced Computing & Communication Technologies, Rohtak, India, 8–9 February 2014; pp. 398–402.
3. Babun, L.; Aksu, H.; Ryan, L.; Akkaya, K.; Bentley, E.S.; Uluagac, A.S. Z-IOT: Passive device-class fingerprinting of zigbee and z-wave iot devices. In Proceedings of the ICC 2020–2020 IEEE International Conference on Communications (ICC), Dublin, Ireland, 7–11 June 2020; pp. 1–7.
4. Anitha, C.; Sivakumar, C.; Rajasekar, V.; Velliangiri, S. Dynamic Tree Routing Protocol with Convex Hull Optimization for Optimal Routing Paths. In Proceedings of the 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 16–18 March 2022; pp. 729–733.
5. Shaukat, K.; Alam, T.M.; Hameed, I.A.; Khan, W.A.; Abbas, N.; Luo, S. A review on security challenges in internet of things (IoT). In Proceedings of the 2021 26th International Conference on Automation and Computing (ICAC), Portsmouth, UK, 2–4 September 2021; pp. 1–6.
6. Liu, Y.; Chen, Y.; Wang, J.; Niu, S.; Liu, D.; Song, H. Zero-bias Deep Neural Network for Quickest RF Signal Surveillance. In Proceedings of the 2021 IEEE International Performance, Computing, and Communications Conference (IPCCC), Austin, TX, USA, 29–31 October 2021; pp. 1–8.
7. Hasan, M.; Mohan, S. Protecting Actuators in Safety-Critical IoT Systems from Control Spoofing Attacks. In Proceedings of the 2nd Workshop on the Internet of Things Security and Privacy—Iot S&P'19, London, UK, 15 November 2019; ISBN 978-1-4503-6838-4/19/11.
8. Damghani, H.; Damghani, L.; Hosseinian, H.; Sharifi, R. Classification of Attacks on IoT. In Proceedings of the 4th International Conference on Combinatorics, Cryptography, Computer Science and Computation, Tehran City, Iran, 20 November 2019.

9. Hijazi, S.; Obaidat, M.S. Address resolution protocol spoofing attacks and security approaches: A survey. *Secur. Priv.* **2019**, *2*, e49. [CrossRef]
10. Madani, P.; Vlajic, N.; Sadeghpour, S. MAC-Layer Spoofing Detection and Prevention in IoT Systems: Randomized Moving Target Approach. In Proceedings of the 2020 Joint Workshop on CPS&IoT Security and Privacy, Virtual Event, 9 November 2020; pp. 71–80.
11. Shi, Y.; Davaslioglu, K.; Sagduyu, Y.E. Generative adversarial network for wireless signal spoofing. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning, Miami, FL, USA, 15–17 May 2019; pp. 55–60.
12. Chua, M.; Balachandran, V.; Kapoor, G.; Weisheng, T. Location Spoofing Detection Enhancement through RSSI Inferred Movement Analysis. In Proceedings of the 2020 Sixth International Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 22–23 February 2020; pp. 1–4.
13. Xiao, L.; Greenstein, L.; Mandayam, N.; Trappe, W. Fingerprints in the ether: Using the physical layer for wireless authentication. In Proceedings of the 2007 IEEE International Conference on Communications, Glasgow, UK, 24–28 June 2007; pp. 4646–4651.
14. Jiang, Z.; Zhao, J.; Li, X.; Han, J.; Xi, W. Rejecting the attack: Source authentication for WIFI management frames using CSI information. In Proceedings of the 2013 IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 2544–2552.
15. Abbas, S.; Talib, M.A.; Ahmed, A.; Khan, F.; Ahmad, S.; Kim, D.H. Blockchain-based authentication in internet of vehicles: A survey. *Sensors* **2021**, *21*, 7927. [CrossRef] [PubMed]
16. Chumchu, P.; Saelim, T.; Sriklauy, C. A new MAC address spoofing detection algorithm using PLCP header. In Proceedings of the International Conference on Information Networking 2011 (ICOIN2011), Kuala Lumpur, Malaysia, 26–28 January 2011; pp. 48–53.
17. de Lima Pinto, E.M.; Lachowski, R.; Pellenz, M.E.; Penna, M.C.; Souza, R.D. A machine learning approach for detecting spoofing attacks in wireless sensor networks. In Proceedings of the 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 16–18 May 2018; pp. 752–758.
18. Mohammadnia, H.; Slimane, S.B. IoT-NETZ: Practical spoofing attack mitigation approach in SDWN network. In Proceedings of the 2020 Seventh International Conference on Software Defined Systems (SDS), Paris, France, 20–23 April 2020; pp. 5–13.
19. Zhang, P.; Nagarajan, S.G.; Nevat, I. Secure location of things (SLOT): Mitigating localization spoofing attacks in the Internet of Things. *IEEE Internet Things J.* **2017**, *4*, 2199–2206. [CrossRef]
20. Jiang, P.; Wu, H.; Wang, C.; Xin, C. Virtual MAC spoofing detection through deep learning. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 20–24 May 2018; pp. 1–6.
21. Wang, N.; Jiao, L.; Wang, P.; Dabaghchian, M.; Zeng, K. Efficient identity spoofing attack detection for IOT in mm-wave and massive mimo 5g communication. In Proceedings of the 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
22. Jiang, P.; Wu, H.; Xin, C. A Channel State Information based Virtual MAC Spoofing Detector. *High-Confid. Comput.* **2022**, *2*, 100067. [CrossRef]
23. Ahmad, S.; Khan, F.; Whangbo, T.K. Performance Evaluation of Topological Infrastructure in Internet-of-Things-Enabled Serious Games, CMC-Computers. *Mater. Contin.* **2022**, *71*, 2653–2666. [CrossRef]
24. Khan, F.; Zahid, M.; Gürüler, H.; Tarımer, İ.; Whangbo, T. An Efficient and Reliable Multicasting for Smart Cities. *Comput. Mater. Contin.* **2022**, *72*, 663–678. [CrossRef]
25. Rahmani, A.M.; Ali, S.; Malik, M.H.; Yousefpoor, E.; Yousefpoor, M.S.; Mousavi, A.; Hosseinzadeh, M. An energy-aware and Q-learning-based area coverage for oil pipeline monitoring systems using sensors and Internet of Things. *Sci. Rep.* **2022**, *12*, 1–17. [CrossRef]
26. Khan, F.; Khan, A.W.; Shah, K.; Qasim, I.; Habib, A. An Algorithmic Approach for Core Election in Mobile Ad-hoc Network. *J. Internet Technol.* **2019**, *20*, 1099–1111.
27. Khan, F.; Khan, A.W.; Khan, S.; Qasim, I.; Habib, A. A Secure Core-Assisted Multicast Routing Protocol in Mobile Ad-Hoc Network. *J. Internet Technol.* **2020**, *21*, 375–383.
28. Khan, F.; Abbas, S.; Khan, S. An efficient and reliable core-assisted multicast routing protocol in mobile Ad-Hoc network. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 231–242. [CrossRef]
29. Delays in Computer Networks | Formulas. Available online: https://www.gatevidyalay.com/delay-in-computer-networks/ (accessed on 17 May 2022).
30. Internal Energy Formula—Definition, Equations, Examples. Available online: https://www.toppr.com/guides/physics-formulas/internal-energy-formula/ (accessed on 25 May 2022).
31. Khan, F.; Ahmad, S.; Gürüler, H.; Cetin, G.; Whangbo, T.; Kim, C.G. An Efficient and Reliable Algorithm for Wireless Sensor Network. *Sensors* **2021**, *21*, 8355. [CrossRef] [PubMed]
32. Ahmad, S.; Mehmood, F.; Khan, F.; Whangbo, T.K. Architecting Intelligent Smart Serious Games for Healthcare Applications: A Technical Perspective. *Sensors* **2022**, *22*, 810. [CrossRef] [PubMed]
33. Malik, A.; Khan, M.Z.; Faisal, M.; Khan, F.; Seo, J.T. An Efficient Dynamic Solution for the Detection and Prevention of Black Hole Attack in VANETs. *Sensors* **2022**, *2*, 1897. [CrossRef]