Hindawi
Security and Communication Networks
Volume 2022, Article ID 4943218, 18 pages
https://doi.org/10.1155/2022/4943218

Research Article

Comparison of Blackhole and Wormhole Attacks in Cloud MANET Enabled IoT for Agricultural Field Monitoring

Tauqeer Safdar Malik,[1] Muhammad Nasir Siddiqui,[1] Muhammad Mateen,[1] Kaleem Razzaq Malik,[1] Song Sun,[2] and Junhao Wen [2]

[1]*Department of Computer Science, Air University Multan Campus, Multan 60000, Pakistan*
[2]*School of Big Data and Software Engineering, Chongqing University, Chongqing 401331, China*

Correspondence should be addressed to Junhao Wen; jhwen@cqu.edu.cn

Received 10 November 2021; Revised 30 December 2021; Accepted 14 March 2022; Published 29 April 2022

Academic Editor: Yuyu Yin

In Mobile Ad hoc Network (MANET) enabled Internet of Things (IoT) agricultural field monitoring, sensor devices are automatically connected and form an independent network that serves as a cloud for many services such as monitoring, securing, and properly maintaining. Cloud-based services in MANET models can prove to be an extremely effective way of smart agricultural functionalities for device-to-device information exchange. Security is a serious issue with Cloud-MANET-based IoT since nodes are scattered, mobile, and lacking centralized administrator, which makes it possible for data tampering and illegal actions on cloud servers. Therefore, these types of networks are more vulnerable to Denial of Service (DoS) attacks such as Blackhole and Wormhole. The MANET Enabled IoT-Agricultural Field Monitoring environment is deployed through a case study. The effect of Blackhole and Wormhole attacks is analyzed using the Ad hoc On-demand Distance Vector (AODV) routing protocol with the help of Network Simulator 3 (NS-3) in order to determine which has the most impact on network performance. We computed performance constraints such as throughput, packet delivery ratio (PDR), end-to-end delay (EED), and Jitter-Sum of preprocessed data gathered with the flow-monitor module of NS-3. The effect of attacks on MANET Enabled IoT-Agricultural Field Monitoring is compared on the varying number of nodes participating in the Cloud-MANET-based IoT network. The throughput and goodput capability of every node is computed through the trace metric package. This method is also highly useful for future Cloud-MANET-Based IoT smart agricultural field security research.

1. Introduction

Cloud MANET-Based IoT is a smart devices platform that combines MANET, Cloud Computing, and IoT. This platform may connect to the cloud and provide cloud-based services to MANET customers by existing smart devices of the IoT system, which handles all the computing, data processing, and resource allocation. Inside the MANET coverage, IoT devices can circulate between one position to another to communicate and share information through cloud servers. Multiple MANETs may link with the same cloud and employ real-time cloud services. Connection of the IoT devices with mobile applications is required to link cloud-based MANET's smart devices to the cloud [1].

The connectivity between the smart devices does not rely on a centralized infrastructure for locating neighboring devices in IoT-MANET platform. The use of cloud-based resources in MANET model for device-to-device connectivity can be a very effective way to improve smart device abilities [2]. Users of smart devices can also use cloud services to reduce the amount of useable data within big data and process videos, text, audio, and images [2]. Farmers working in the agriculture sector can use the data obtained from the farming to analyze, monitor, and make a decision. Farmers may use mobile devices, sensors, and scanners to access a variety of cloud-based services for IoT devices working in MANET environment [3].

Mobile Ad hoc Network sets up a network with their neighbors' smart devices and transfers data to another device just like a router. MANET and Cloud computing make up the cloud-MANET platform for smart devices. This system will connect to and provide cloud resources to MANET users by the smart devices, which manages all calculations, management of resources, and data handling. Smart devices have the potential to switch between one place to another, and Multiple MANETs can link to a certain cloud and use run-time cloud services. To connect MANET's smart devices to the cloud, interconnection with mobile applications is required. The MANET framework of smart devices with local connectivity can perform best when connected to the cloud, but it fails when connected to an existing wired networking infrastructure. An entry point, equivalent to gateways, would be needed for operating in wireless and wired networks [4].

In order to join a smart device to some other device throughout the cloud-MANET network, each IoT smart device must have been uniformly equipped with resources such as memory, connectivity, and energy [5]. For routing purpose, cloud-based IoT devices linked to MANET nodes and IoT nodes in MANETs use MANET Routing Protocols. The IoT devices linked to MANET in cloud-based network for agricultural field monitoring must ensure the availability and connectivity at all times. The availability in terms of security is most important in monitoring application for an agricultural field, so that a farmer can get the real-time data collection and decision making. The cloud-based data servers can work very efficiently to ensure the availability of up-to-date information for real-time decision making [6]. Therefore, it is extremely important to implement a cloud MANET enabled IoT network for monitoring of agricultural field. The IoT nodes participating in cloud-based MANET for monitoring agricultural fields are much susceptible to availability attacks such as Denial of Service (DoS) attacks due to their very limited capability of memory, computing, and energy. The blackhole and wormhole attacks are very known and dangerous in DoS attacks on availability in MANET. The availability of real-time data is critical in case of monitoring of agricultural field on cloud MANET enabled IoT network. The data centers provide the best computing facility for any case of emergency, and IoT nodes in MANETs have been equipped with the Internet and low power and lossy network (LLN) topology, for routing protocol standard (RPL) [7]. The existing security and limited hardware resources in RPL are having deficiency in defense against numerous security attacks. Gateway routers linked with IoT devices in MANETs must be consistent and valid to protect MANET routing protocols and Internet routing protocols [8].

The communications in cloud-based MANET are carried through the different kind of reactive and proactive routing protocols such as Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) to find nearest path from source to destination node [9]. The cloud-based MANET is used in different fields such as in IoT, Industrial Internet of Things (IIoT), Medical Services, Security, Commercial, and Agriculture Sectors [10]. We used AODV routing protocol that establishes a path from source node to destination node upon request in cloud MANET enabled IoT for monitoring of agricultural field. The physical manipulation like stealing or attacks by insects and animals, as well as modification in physical address or connection, makes smart devices defenseless in agricultural field monitoring solution based on cloud MANET enabled IoT. The different types of Denial of Service (DOS), congestion, and forwarding attacks can affect the common gateway, providing the services of cloud-based MANET to the end user [11]. The cloud-based MANET routing protocols are not secure, and therefore, the malicious node can find the drawbacks and attack on network, because sensor devices are widely dispersed, and they are vulnerable to malicious cyberattacks [12].

In this paper, we have simulated blackhole and wormhole attack to test the functionality of Cloud MANET enabled IoT for monitoring agricultural field with and without DoS attacks for monitoring the agricultural field as shown in Figure 1. On the base of performance metrics, the main contribution of this paper is to:

(i) Compare the effect of blackhole and wormhole attacks on the performance of the Cloud MANET enabled IoT network for monitoring of agricultural field.

(ii) Determine either blackhole attack or wormhole attack is more harmful and affecting the network performance of cloud MANET enabled IoT network.

To simulate results, we have utilized the Network Simulator-3 (NS-3), which is very famous as an open-source tool. Following the outcomes of the tests, we evaluated network performance by using metrics like average throughput, average end-to-end delay, average packet delivery ratio, and average jitter sum delay with reference to the total number of nodes within the network. We also have evaluated goodput and throughput of every node that are present in the network under with and without blackhole and wormhole attacks in cloud MANET enabled IoT network for agricultural field monitoring.

The rest of the paper is arranged as follows: the related work is discussed in the upcoming section for the literature review and effectiveness of the research. The material and methodology are followed by literature review in the next section with detailed graphical view and methodological model of Cloud MANET enabled IoT network for monitoring of an agricultural field. The next section discusses the simulation setup for varying number of IoT nodes participating in MANET enabled IoT network, followed by a complete section of results and analysis of the implemented setup. Finally, conclusion and recommendations for future work are given in last section.

2. Related Work

With the rapid deployment of Internet of Things (IoT) in the smart agriculture, it is modern and essential to cope it with future technology Cloud-based MANET. The innovation-driven architecture of cloud-based MANET is related to the

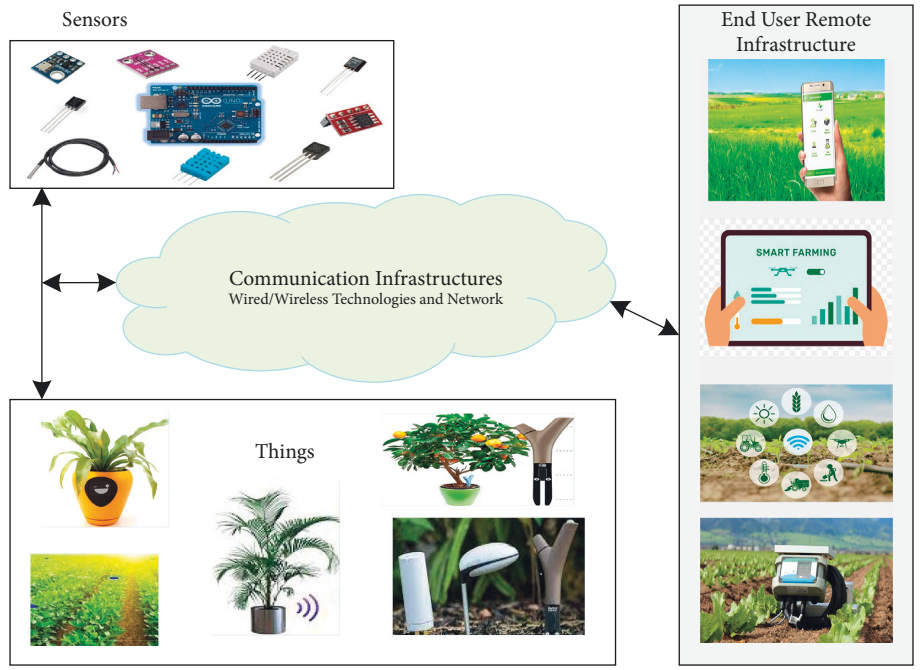


Figure 1: Graphical representation of agricultural field monitoring using MANET enabled IoT network.

monitoring solutions and is subject to security risks and privacy issues for an excessive number of IoT devices [13]. There are many solutions of Cloud-based MANET, which enable the agricultural monitoring solutions and highlights the dire need of IoT based devices to be equipped with these technologies. The cloud computing-based models such as Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) are heterogeneous in adopting the virtualization of different technologies [14]. Due to the heterogeneity and diversity of applications, especially the development and emergence of IoT, they offer more challenges and security threats in cloud environments [15]. Therefore, Cloud enabled MANET in Agricultural monitoring has massive data transmission on the network links, which not only affects the energy consumption in the cloud environment, but also increases the security risks. A cloud-based data center for MANET should facilitate the users with privacy and availability at all times while working in agricultural monitoring application. The cloud-based MANET should enable the user the better network configuration and availability of service at all times when monitoring any special task to ensure the services of the users especially in cyber-physical systems [16]. In the literature, there are various types of attacks discussed on availability in MANET, but there is still infancy to detect and prevent such attacks especially in cloud-based networks. The Denial of Service (DoS) attacks are very popular on availability and many solutions presented for its detection in MANET, and it is very important to analyze the effect of these attacks in cloud-based MANET especially in IoT devices. In [17], the authors presented a scenario of cooperative blackhole attack, one of the most dangerous DoS attacks, in Wireless Sensor Network (WSN) and MANET as a defenseless attack. A cooperative blackhole attack contains a large number of malicious nodes working with trusted users, which affect the performance of IoT enabled MANET [18]. The security and privacy of IoT challenges should be verified by using formal methods, such as DoS, theorem-proving, and formal testing [19]. An algorithm for determining the safer path in case of blackhole attack between the sender and receiver is presented in [20] for secure and efficient communication by evaluating each route and channel, but this reliable path is for fixed locations.

Similarly, the detection of the wormhole attack not only reveals the Internet of Things (IoT) network, but also identifies the victim nodes undergoing remotely controlled [20]. There are other attacks too, such as Sybil attack, HELLO flood attack, sinkhole attack, and spoofing attack, which are caused by the wormhole attack. Therefore, the wormhole attack should be explored and simulated in the cloud-based MANET especially for IoT network, in which heterogeneous technologies were used, which could be causes of software and hardware exploitation. Later, in [21], the authors developed a system that focused on the variety of cyberattacks in IoT and Industrial IoT networks caused by blackhole attacks established on Routing Protocol for Low-power and Lossy Networks (RPL). The malevolent network nodes modify the path of packets and immediately send it through a different route than the one specified for the wormhole and blackhole nodes [22]. It may result in illegal data packet observation or even small amount of packet loss in IoT networks based on cloud [23]. This is known as a black hole attack when the Packet Delivery Ratio (PDR) exceeds a certain threshold, but the overall throughput of the network is not observed in cloud-based MANET.

In [24], the authors worked on MANET enabled IoT network and simulated the effects of Sybil attack in on network performance using routing protocol RPL. It can

first and foremost allow a dynamic scope of movement between nodes in the network, which is becoming increasingly important for real-time applications. But on the other hand, due to its resource constraints, RPL is extremely prone to numerous security attacks such as blackhole and wormhole attacks [25].

The IoT devices especially sensors are viewed as a significant security risk because of its modification that can be used as source nodes for DoS attacks [22]. Furthermore, there are many other resource limitations in cloud-MANET enabled IoT network such as less memory, conversation capacity, and minimum energy utilization to execute large and reined algorithms in IoT devices [26]. The safety and location for the position of information, as well as IoT empower location-based services used mostly for smart agriculture, are vulnerable to threats like device capturing [27]. An attacker can easily spoof an IoT device and retrieve the cryptographic design as well as having its uncontrolled usages to get all the information contained in the cache of device [28]. Extra demands for edge device functionalities may also be imposed in automation of IoT nodes for smart agricultural functionalities [29]. However, the significant risk that may be in agricultural as well as other industrial environment due to these weaknesses needs to be investigated more in the upcoming works [30].

The literature stated various levels of the IoT environment and highlighted many security concerns that must be researched and resolved. Inadequate protection may result in loss of data and violation of privacy and obtain raw data regarding on-field criteria and other important intellectual properties [31]. The DoS attacks, those that can come in the form of signal cancelling or jamming, are highly vulnerable to wireless links and put accessibility of a IoT device at risk in cloud-based MANET. Although spread spectrum techniques could be employed to prevent wireless jamming, there is still no feasible solution for preventing DoS attacks for IoT devices with limited resources [32].

Due to restricted memory, connectivity capacity, and low power consumption, complicated and refined algorithms are difficult to be incorporated in IoT devices [33]. The gateway can also be targeted by congestion, DoS, and routing attacks. Furthermore, cloud servers are vulnerable to data modification and unauthorized operations, which can disrupt operations in the agricultural farms. Session hijacking, server access control and database problems, and login misuse are some of the other security issues that can threaten cloud platform in the presence of DoS attacks [34]. Therefore, to secure the cloud MANET enabled IoT network from the DoS attacks such as blackhole and wormhole attacks in a limited resources of hardware and software, first of all, there must be a proper comparison of these attacks on network performance in monitoring of agricultural fields to prevent them. Hence, there is a need to check which DoS attack is more vulnerable for the overall performance of cloud MANET enabled IoT network for a limited capacity of IoT devices used in monitoring of agricultural fields.

3. Materials and Methods

The smart agricultural filed monitoring is based on not only agricultural knowledge to support the deployment of a variety of intelligent applications, but also the expertise of the IoT devices, wireless technology, cloud computing, and intelligent systems. Figure 2 depicts the materials required to implement the cloud MANET enabled IoT network for monitoring of an agricultural field. IoT nodes are used as sensors to calculate weather, levels of soil moisture, temperature, soil fertility, and soil Ph level to assess whether each field has the best growing season and cultivation areas. The IoT devices are part of the network, performing different tasks in the agricultural field monitoring as shown in Figure 2. The attacker nodes are circled red in the network, which are causing the blackhole and wormhole attacks to make network unavailable for its services. Due to these attacks, the cloud-based MANET may not take the real-time decisions in case of unavailability. The data collection on cloud is delayed and partially received due to the blackhole and wormhole attack on IoT devices participating in monitoring of agricultural field. The cloud computing environment facilitates the traditional computing platforms to avoid the maintaining cost and investments in hardware by users, usually in terms of virtual machines. This new computing mode can enhance the efficiency, productivity, and scalability of increasingly more applications such as earthquake prediction, weather forecasting, and monitoring of smart agriculture. The diversity of IoT devices and its applications in smart agriculture brings more concerns and opportunities for real-time decision making in the cloud [16]. This is essential for gaining the most output of the production while minimizing loss of environmental resources [29]. As a result, different kinds of sensors are used in conjunction with other controller equipment to gather information in order to protect agricultural areas [30]. The Global Positioning System (GPS) is a space-based navigation system that offers a real-time features and positioning information across all weather conditions for monitoring. As a result, GPS helps farmers in increasing development and controlling land resources [31]. One of the really significant considerations in ensuring the efficiency of an agricultural commodity is the protection of such areas. Farmers can quickly implement video monitoring systems in their agricultural regions and provide consumers with really fresh and high-quality products at the end of the day, while securing livestock, vehicles, and services from damage and misuse. As a result, a web camera is an excellent tool for accomplishing this mission because it can catch photographs of any dangerous rodent within seconds when Infrared sensors sense motion [28]. The IoT nodes can communicate with the cloud servers directly or by a gateway, whereas digital images can be recorded by camera nodes through field cameras, drones, and sometimes satellite pictures. The connectivity of IoT nodes with the cloud servers is maintained for the purpose of remote visualization and smart application creation. Remote users may be using either workstations or/and smart devices to acquire the data and smart applications, which can be used to acquire the cloud

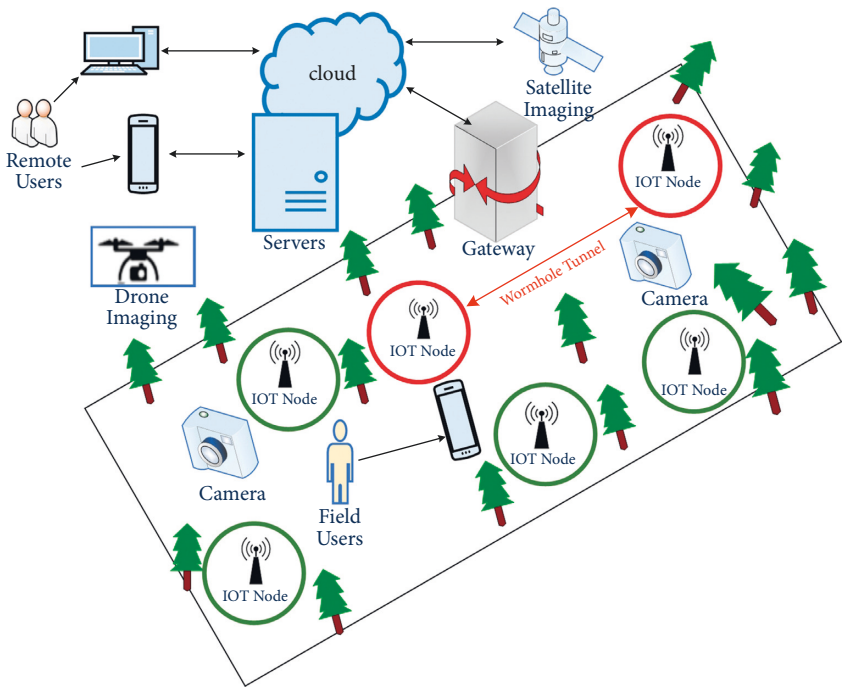


Figure 2: Cloud MANET enabled IoT Deployment for the Agricultural Field Monitoring.

for field users. Because of this, there is a possibility of different kind of attacks that not only destroy the overall network performance, but also make it unavailable for its services. The service of remote field monitoring of agricultural field requires the availability at all time and detects any malicious activity from the cloud-based MANET.

The state-of-the-art methodology is presented to implement and analyze the effect of blackhole and wormhole attacks in cloud MANET enabled IoT network for monitoring of an agricultural field. The enactment of blackhole and wormhole attacks in the MANET enabled IoT network requires modifying the working of existing Ad hoc On-demand Distance Vector (AODV) routing protocol. IoT Nodes are mobile in MANET, and AODV provides facility to these nodes to find route instantaneously that is necessary for communication. The effect of blackhole and wormhole attacks is simulated separately, and its detailed method is presented in the next subsections, respectively.

3.1. Blackhole Attack Execution in Cloud MANET Enabled IoT Network. The blackhole attack is the type of a of Denial-of-Service (DoS) attack, and it affects the availability of a user by disrupting the network layer, which serves as routing purposes in cloud MANET enabled IoT network. An attacker node changes the normal behavior of routing protocol, and the victim node assumes that it has a valid route to transmit packets to destination. During the route-finding process, a source node broadcasts RREQ to all its neighboring nodes. When attacker node receives this request, it sends RREP message to source node with large sequence number and hop count 1 [35]. Upon reception of these packets by attacker node, it drops all the packets and does not forward them to the destination IoT node as shown in Figure 3, which makes the data unavailable for cloud MANET.

IoT node S is the source node, and IoT node *D* is the destination node. The source node sends RREQ message to all its neighbors A, B, and C. The IoT Node B is an attacker node that sends RREP message to source node S by increasing sequence number and minimizing hop count earlier than IoT Node A and C. The source (victim) node S decides that node B (attacker node) provides valid/fast route to destination and sends data packets to it. Upon receiving packets, node B drops all the packets and does not forward them to the destination node D. Hence, the blackhole attacker makes the user unavailable to its services.

The blackhole attacks can be categorized as single and collaborative blackhole attacks. When one single node in the network acts as an attacker node to make unavailable the victim node as shown in Figure 3, it is categorized as single blackhole attack, whereas when more than one attacker node collaboratively attacks as shown in Figure 4, it is called collaborative blackhole attack [36].

Here, two attacker nodes B and C make unavailable node S and drop data packets as received from source node. Both blackhole scenarios can be implemented and executed in the cloud MANET enabled IoT network as presented in Figure 5. The AODV routing protocol is modified to execute the blackhole attacks in single or collaborative mode using Algorithm 1 in cloud MANET enabled IoT network. The mathematical model is presented in Figure 6 to compare the results.

3.2. Wormhole Attack Execution in Cloud MANET Enabled IoT Network. Usually, a wormhole attack is initiated by two or more malevolent IoT nodes using a special path called

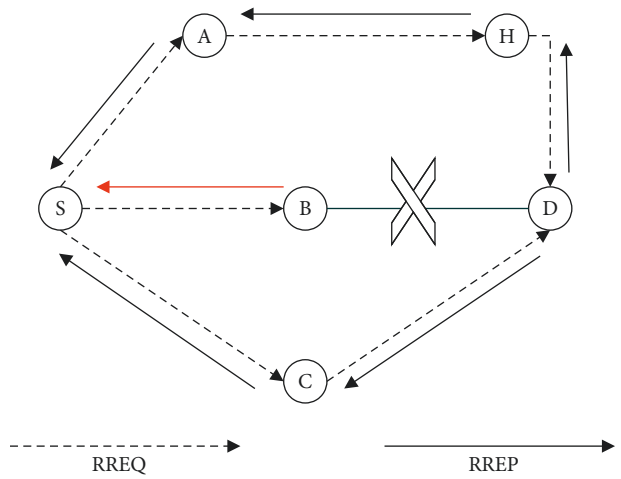


Figure 3: Blackhole attack in AODV routing of MANET enabled IoT.

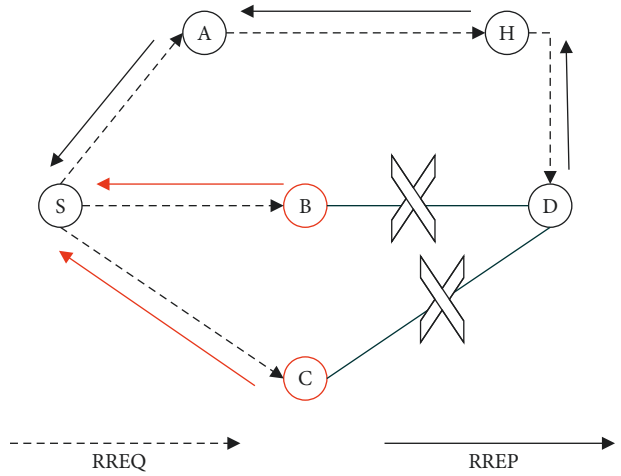


Figure 4: Collaborative blackhole attack in AODV routing of MANET enabled IoT.

tunnel among them in cloud MANET enabled IoT network. Data packets received by any one of the malevolent nodes are sent to the other malevolent node by using this tunnel. The malevolent IoT nodes may send data packets to each other in many numbers of times using this tunnel and due to this, the battery of other nodes becomes overextended, and the IoT device services of monitoring the agricultural field were affected [36].

The wormhole attack is depicted in Figure 7, in which the two IoT attacker nodes are represented as *X* and Y in MANET enabled IoT network. In path finding process, source IoT node **S** transmits RREQ to its neighbors A and *X* where *X* is the first end of worm tunnel, which is connected with second end of worm tunnel Y. Y sends RREQ to its neighbor C-G to reach destination node IoT D. Destination (final) node transmits RREP message to source (initial) IoT node using the path of worm tunnel, and source IoT node is still waiting for the RREP message, which makes IoT node unavailable for the services of cloud MANET enabled IoT network. This wormhole tunnel implementation and execution is used in cloud MANET enabled IoT network as shown in Figure 8.

On another end, if RREQ request reaches node Y, then it forms a fast link between Y and *X* and the destination IoT node sends RREP to source node using different path as shown in Figure 9. Because of this, the energy of other nodes is exhausted, and the attacker nodes drop the packets destined for cloud MANET enabled IoT devices. The complete changes of AODV routing protocol to implement wormhole attack in cloud MANET enabled IoT network are presented in Algorithm 2, and the mathematical model of performance metrices used is shown in Figure 6.

3.3. Simulations. The accessibility of a tool for Internet of Things (IoT) or wireless network simulation is one of the primary facilitators for fast development in academia. Chernyshe et al. provide a complete set of simulators utilized in recent research for MANET-based IoT networks [36]. One of them, a very common utilized simulator for cloud MANET

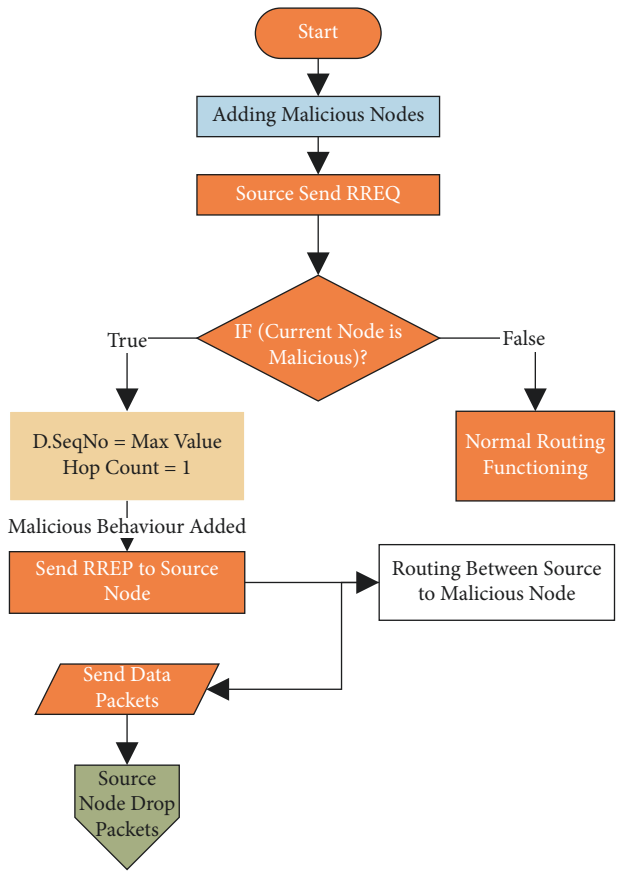


Figure 5: Implementation of a blackhole Attack by modification of AODV Routing Protocol.

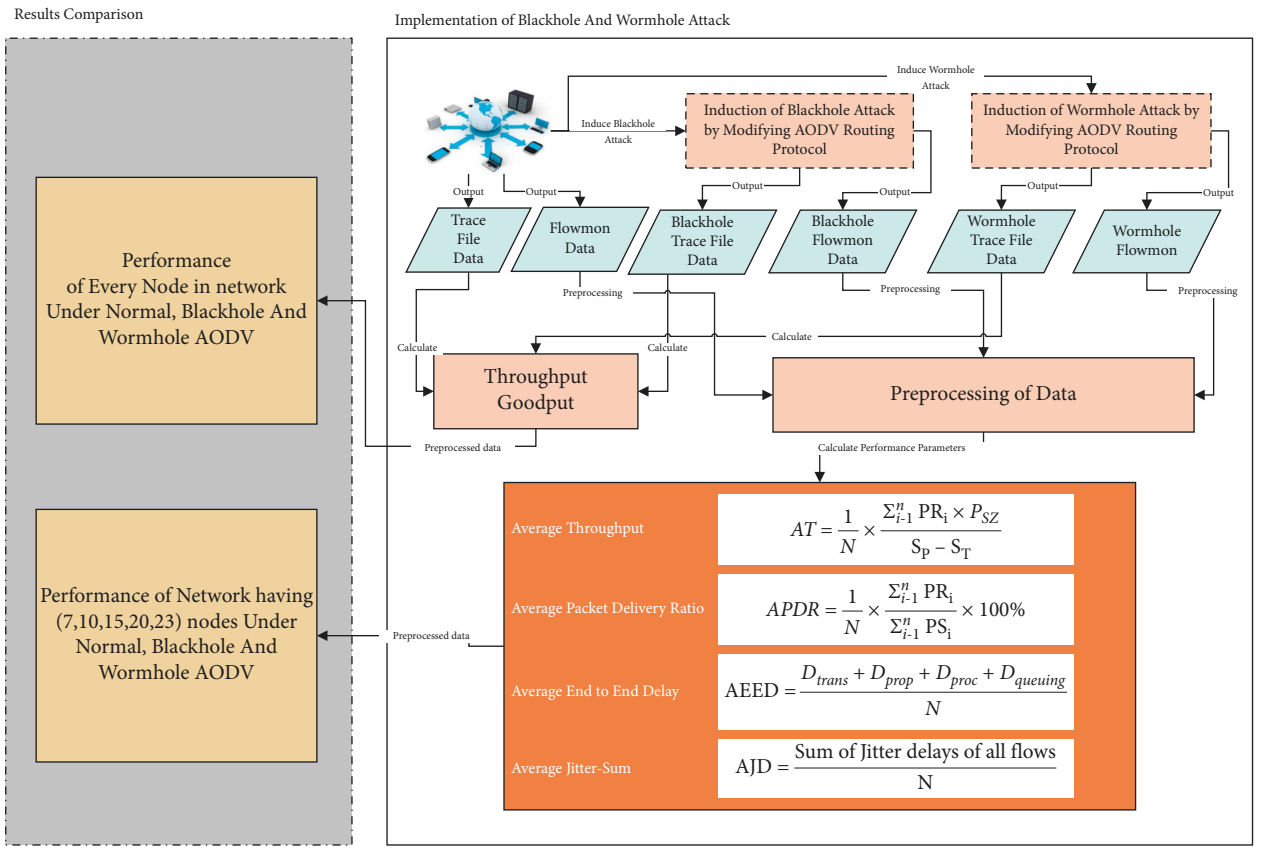


Figure 6: The overall methodology for comparative analysis of blackhole and wormhole attacks.

Step 1: Start: cloud MANET enabled IoT Network without attacker nodes
Step 2: Add one or more IoT attacker node/s in the cloud MANET enabled IoT network.
Step 3: Source node transmits Rout Request (RREQ) message to every neighbor (cloud MANET Enabled IoT) node.
Step 4: **if (existing node attacker?)**
Enlarge sequence number with big value and set hop count 1.
Attacker node transmits Route Reply (RREP) to source node.
Build route among the Originating node and the attacker node.
Forward data packets from originating node to attacker node.
Attacker node will drop all the packets.
Else
AODV Routing Protocol will execute its tasks as usual.
End if
Step 5: Stop

Algorithm 1: Implementation of blockhole attack in cloud MANET Enabled IoT Network.

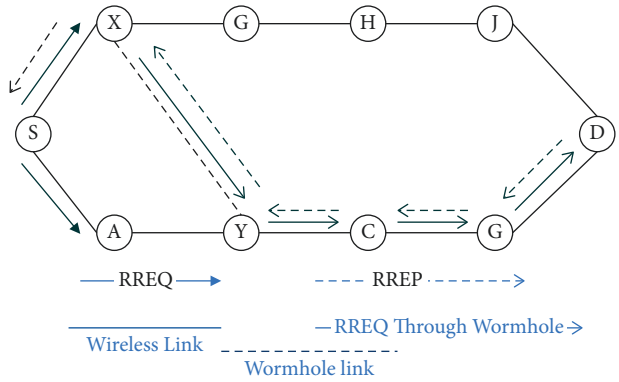


Figure 7: Wormhole Attack in AODV Routing of MANET enabled IoT.

enabled IoT research, is NS-3, an open-source simulator [36]. A network of varying number of IoT nodes participating in cloud MANET enabled IoT network is simulated in Network Simulator-3 (NS-3) and the cloud-based data collected during the monitoring of agricultural field using Flowmon module of NS-3. The trace file data is obtained for throughput and goodput of each node by using trace metric package of NS-3 [37]. Three numbers of blockhole IoT attacker nodes with one wormhole tunnel are used for varying number of IoT nodes participating in cloud MANET enabled IoT network for agricultural field monitoring. The mathematical model for calculating of throughput (TP), end-to-end delay (EED), packet delivery ratio (PDR), and jitter sum (JT) as performance metrics is shown in Figure 6. The results of throughput and goodput are compared to determine the effect of individual attack on cloud MANET enabled IoT network by analyzing the trace file data obtained from the cloud in trace metric module of NS-3. The overall simulation parameters are presented in Table 1.

The simulation setups of cloud MANET enabled IoT network of having different number of IoT-nodes participating in monitoring of an agricultural field are depicted in Figures 10–14. The network area (field) without any attack is represented in (a) part of every Figure and in (b) part of each figure; there are 3 malicious nodes with black color that caused the blackhole attacks shown. Finally, the field with wormhole attack is shown in (c) part of each figure, in which there are 2 malicious nodes with black color. This varying number of IoT nodes is implemented as monitoring devices in agricultural fields to collect the data and make it available on the cloud to make real-time decisions for different purposes [38]. The real-time data is unavailable due to the blackhole and wormhole attacks, and it affects the performance of network performance in terms of throughput, EED, PDR, and JT.

4. Results and Analysis

The results are analyzed and compared on the performance metrics such as Throughput (TH), Packet Delivery Ratio (PDR), End-to-End Delay (EED), Jitter-Sum (JS), and Goodput (GP). The effect of blackhole and wormhole attacks in cloud MANET enabled IoT network is analyzed under three scenarios such as without any attack and with blackhole attack and wormhole attack. The attacks are compared and determined upon the throughput and goodput for varying number of IoT nodes participating in cloud MANET enabled IoT network.

4.1. Effect of Blackhole and Wormhole Attacks on Performance Metrices. The effect of blackhole and wormhole attacks on throughput is shown in Figure 15 for normal operation of network and with attacks of wormhole and blackhole on different IoT nodes participating in cloud MANET enabled

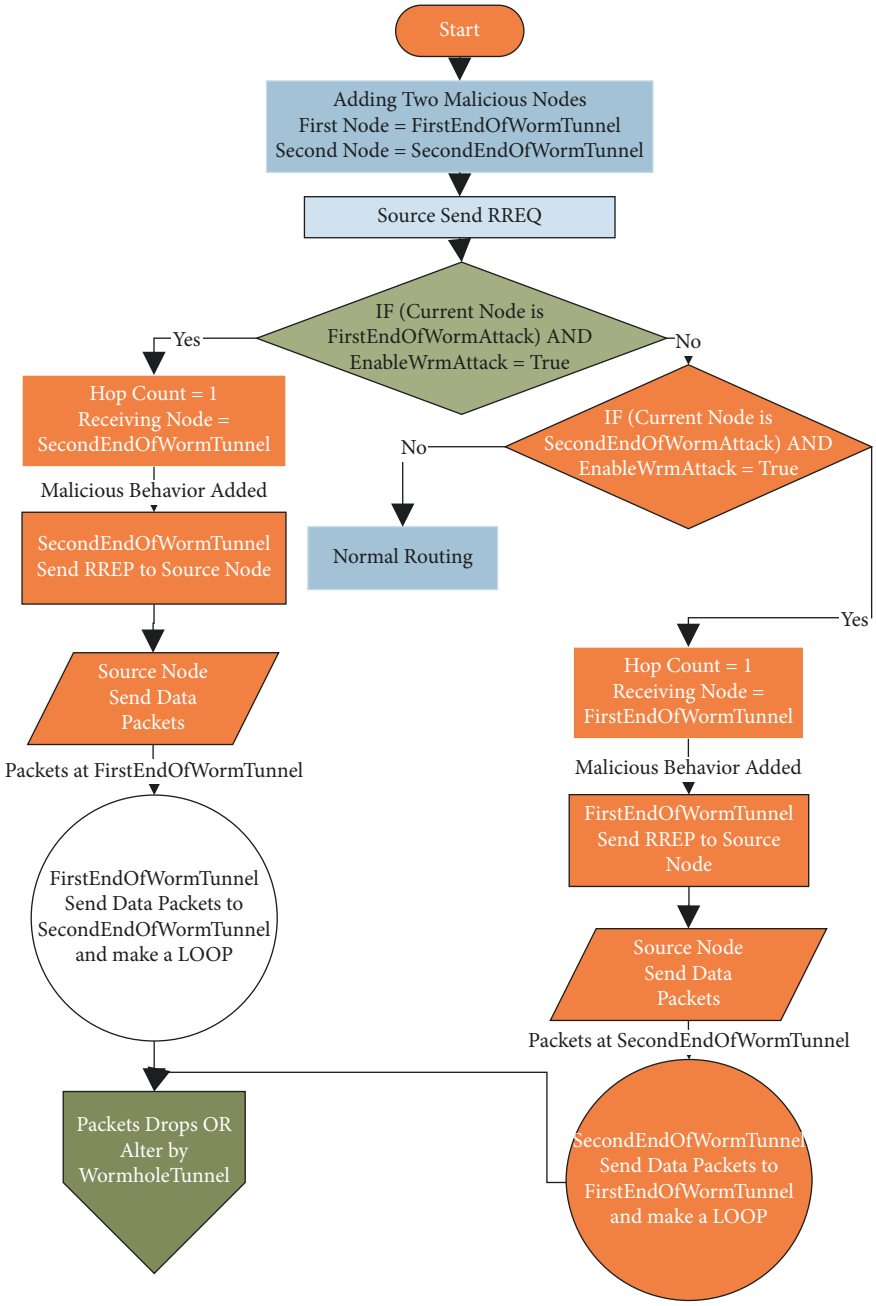


Figure 8: Flowchart implementation of a wormhole attack by modification of AODV routing protocol.

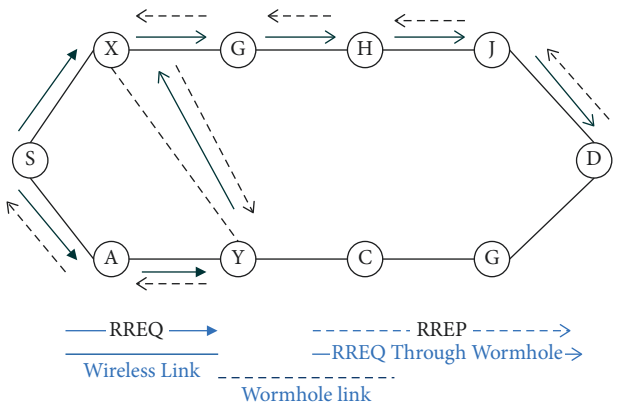


Figure 9: Wormhole Attack using fast link in AODV Routing of MANET enabled IoT.

Step 1: Start: cloud MANET enabled IoT Network without attacker nodes
Step 2: Add two attacker nodes in the cloud MANET enabled IoT network.
Step 3: Set First attacker node as FirstEndOfWormTunnel and second attacker node SecondEndOfWormTunnel
Step 4: Source Node transmits Rout Request (RREQ) message to every neighbor (cloud MANET Enabled IoT) node.
Step 5: **if (EnableWrmAttack is TRUE andand Node is FirstEndOfWormTunnel?)**
Set hop count to 1.
Set ScondEndOfWormTunnel as receiving node and form a fast tunnel
ScondEndOfWormTunnel transmits Rout Request (RREQ) message to its neighbor nodes.
Destination node transmits Route Reply (RREP) message to source node using prearranged Path.
Source node send packets to destination node using prearranged path.
When packets reach at FirstEndOfWormTunnel, it forwards it to SecondEndOfWormTunnel
Else if (EnableWrmAttack is TRUE andand Node is SecondEndOfWormTunnel?)
Set hop count to 1.
Set FirstEndOfWormTunnel as receiving node and form a Fast tunnel.
FirstEndOfWormTunnel transmits Route Request (RREQ) message to its neighbors' nodes.
Destination node transmit Route Reply (RREP) message to source node using predefined Path.
Source node Forward data packets to destination node using prearranged path.
When packets reach at SecondEndOfWormTunnel, it forwards it to FirstEndOfWormTunnel, and start reiterating this process
All Packets drops or change by wormhole nodes.
Else
AODV Routing Protocol execute its tasks as usual.
End if
End if
Step 6: Stop

Algorithm 2: Implementation of wormhole attack in cloud MANET Enabled IoT Network.

Table 1: Simulation parameters.

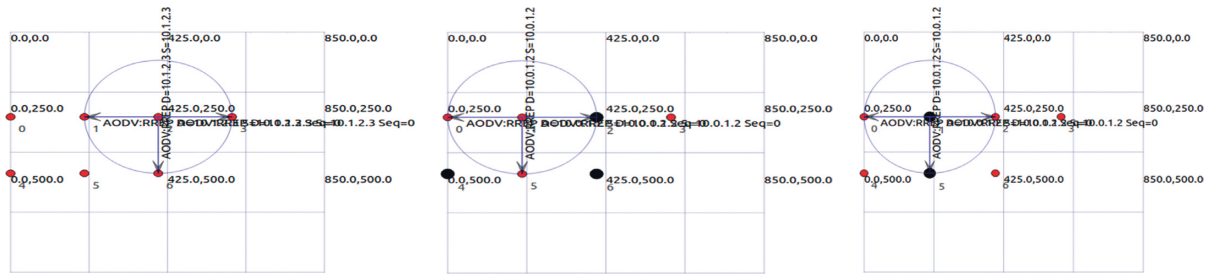
Network parameters	Values
Simulator	NS-3
Platform	Ubuntu 16.04
Simulation time	100 sec
Number of nodes	7, 10, 15, 20, 23
Number of blackhole nodes	3
Traffic	CBR (constant bit rate)
Transmission speed	250 kbps
Transmission rang	250 m ∗ 250 m
Packet size	512 bytes
Routing protocol	AODV
Transport protocol	UDP
Physical layer	DLT_IEEE802_11
MAC layer	802.11 b

IoT network. The graph shows that the average throughput declines steadily as the number of cloud MANET enabled IoT nodes increases due to the network activities of every IoT node. The average throughput for normal working (without attack) on cloud MANET enabled IoT network is 89 kilobits per second in the start and rapidly declines and reaches 29 kilobits per second. The average throughput drops much in case of blackhole attacker node and starts with 19 kilobits per second and declines and decreases faster with increment in the number of IoT nodes and reaches 8.5 kilobits per second. Finally, it is much worse in the presence of wormhole attack and reduces to 1.5 kilobits per second with the increment of number of IoT nodes as shown in Figure 15.

Similarly, the average packet delivery ratio (PDR) of MANET enabled IoT network remains the same in case of normal operation (without attack) with the increment in number of IoT nodes as shown in Figure 16. On the other hand, the average PDR is much worse and extremely less in case of a lesser number of IoT nodes participating in cloud MANET enabled IoT network in the presence of blackhole attack due to less choices of routing decisions, whereas this is not the case of wormhole attack as it starts with a lesser number of IoT nodes, and the average PDR is much better than blackhole attack and decreases with the increasing number of IoT nodes. Hence, the cloud MANET enabled IoT network is not giving a good average PDR in case of blackhole attack when the number of participating nodes in MANET enabled IoT is lesser as shown in Figure 16.

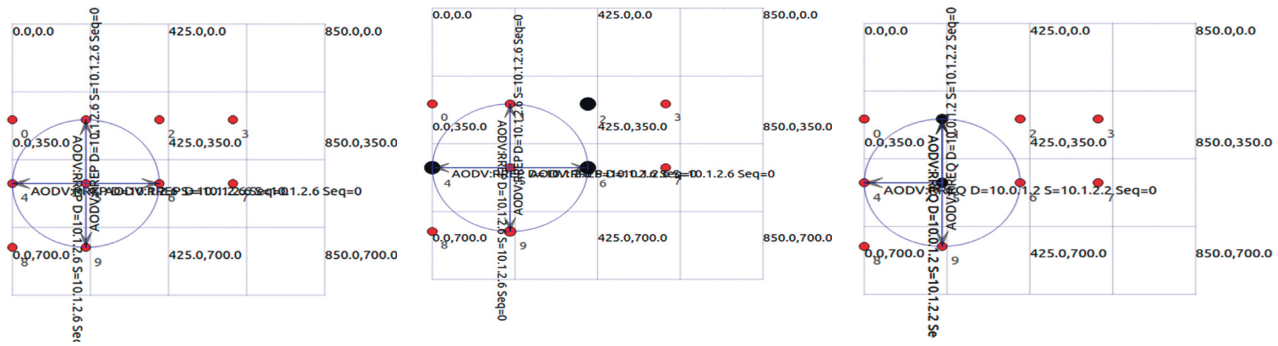
The MANET enabled IoT network surprisingly behaves the same for average End-to-end delay (EED) and average Jitter-Sum (JS) results as shown in Figures 17 and 18. It is shown that the average EED and average JS increase with the increment in the number of IoT nodes in the presence of blackhole attack, and this is even worse in the presence of wormhole attack.

4.2. The Harmfulness of Blackhole and Wormhole Attacks. In this section, the performance of cloud MANET enabled IoT network is compared in terms of throughput (TP) and goodput (GP) for varying number of attacker and victim IoT nodes to determine the harmfulness of blackhole and wormhole attacks and discussed for varying number of nodes participating in monitoring of agricultural filed. The TP refers to the total amount of data that flows across a link, regardless of whether it is beneficial or not, whereas GP is only concerned with useful data.



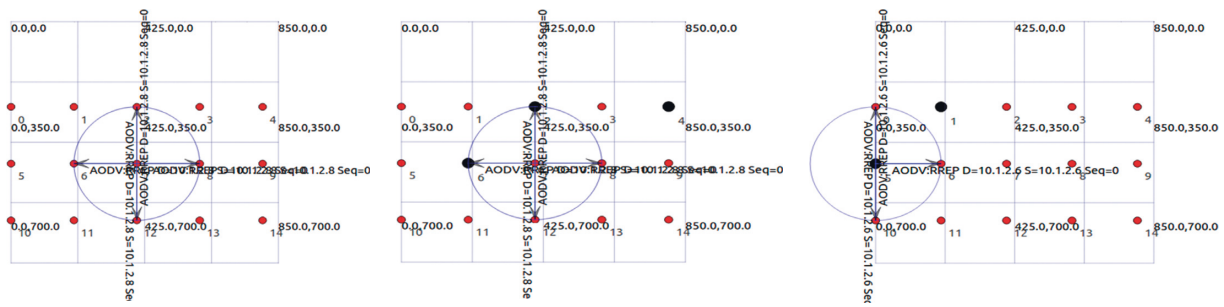
(a) (b) (c)

Figure 10: Smart Agri-Field with 7 number of MANET enabled IoT nodes.



(a) (b) (c)

Figure 11: Smart Agri-Field with 10 number of MANET enabled IoT nodes.



(a) (b) (c)

Figure 12: Smart Agri-Field with 15 number of MANET enabled IoT nodes.

4.2.1. 7 Cloud MANET Enabled IoT Nodes. The graph in Figure 19 shows that the TP of IoT nodes in normal operations and blackhole attack situation stays the same, whereas, in case of wormhole attack, it is very high in the start and drops thereafter rapidly and reaches the same level as in normal operation of cloud MANET enabled IoT network. The graph of GP demonstrates that the IoT nodes performing normal operations (without attack) and with blackhole as well as for wormhole attack are having very good GP in the start, but they reach zero as the number of nodes increases in case of blackhole and wormhole attacks.

The TP contains unwanted data such as data retransmissions and overhead and protocol headers, which are excluded in case of GP. That is why its value is large on every IoT node as compared to the GP. On the other hand, due to tunneling of packet between two attacker nodes, TP of every IoT node is more in case of wormhole attack as compared to blackhole attack.

4.2.2. 10 Cloud MANET Enabled IoT Nodes. Figure 20 illustrates that the overall TP of every IoT node is high in case of wormhole attack as compared to the normal operation (without attack) and in case of blackhole attack. This is because of the presence of wormhole tunnel on both sides, and it provides much better communication for cloud MANET enabled IoT network. The graph of GP shows that the GP of some IoT nodes is higher than that of all other IoT nodes for normal operation, blackhole, and wormhole attacks due to data retransmission and protocol overhead. The

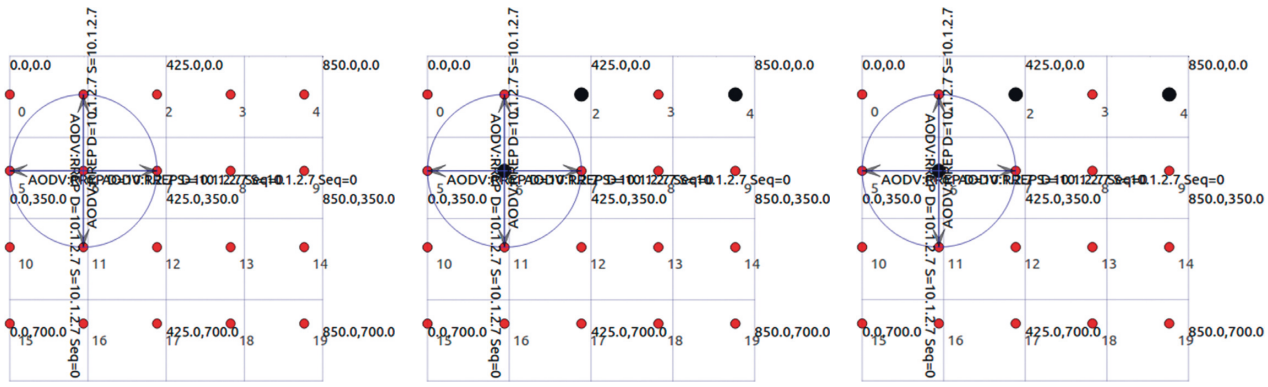


Figure 13: Smart Agri-Field with 20 number of MANET enabled IoT nodes.

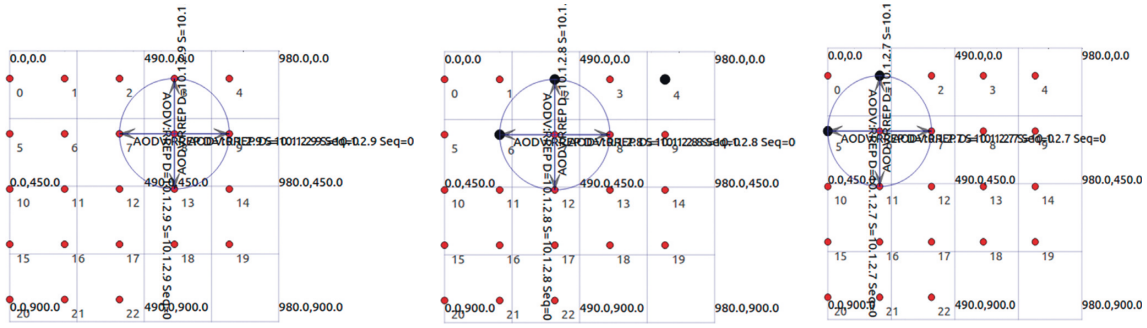


Figure 14: Smart Agri-Field with 23 number of MANET enabled IoT nodes.

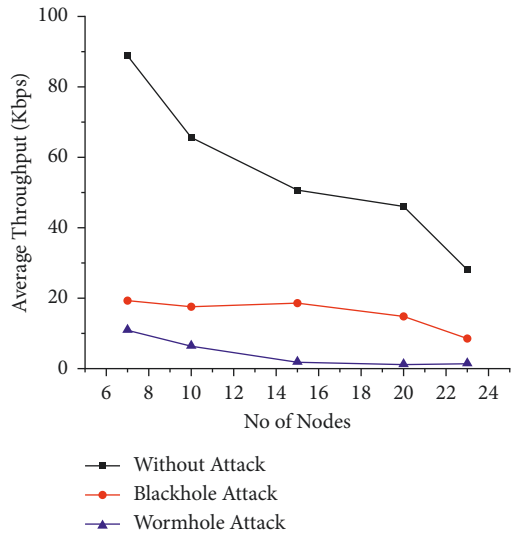


Figure 15: Number of MANET enabled IoT nodes V/S average throughput.

TP value for every IoT node is more as compared to the GP because most of time is consumed in tunneling of data packets.

4.2.3. 15 Cloud MANET Enabled IoT Nodes. The TP graph in Figure 21 shows that the TP remains high for nearly all IoT nodes in case of wormhole attack as compared to other

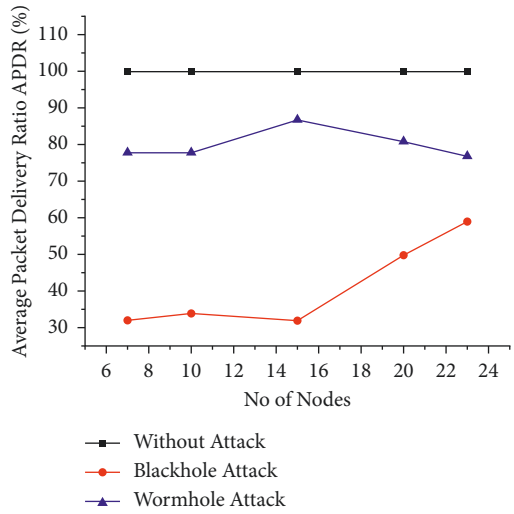


Figure 16: Number of MANET enabled IoT nodes V/S average packet delivery ratio.

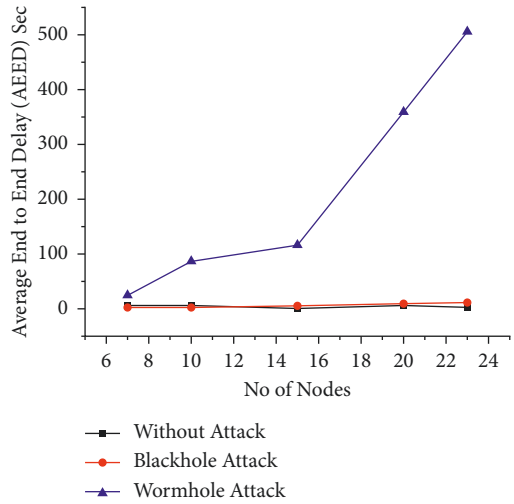


Figure 17: Number of MANET enabled IoT nodes vs average end to end delay.

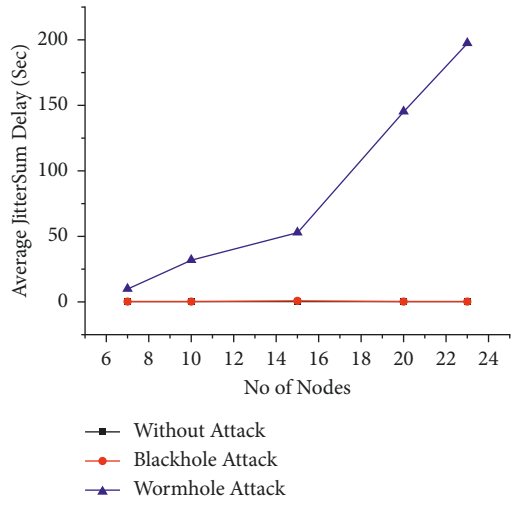


Figure 18: Number of MANET enabled IoT nodes vs average jitter-sum delay.

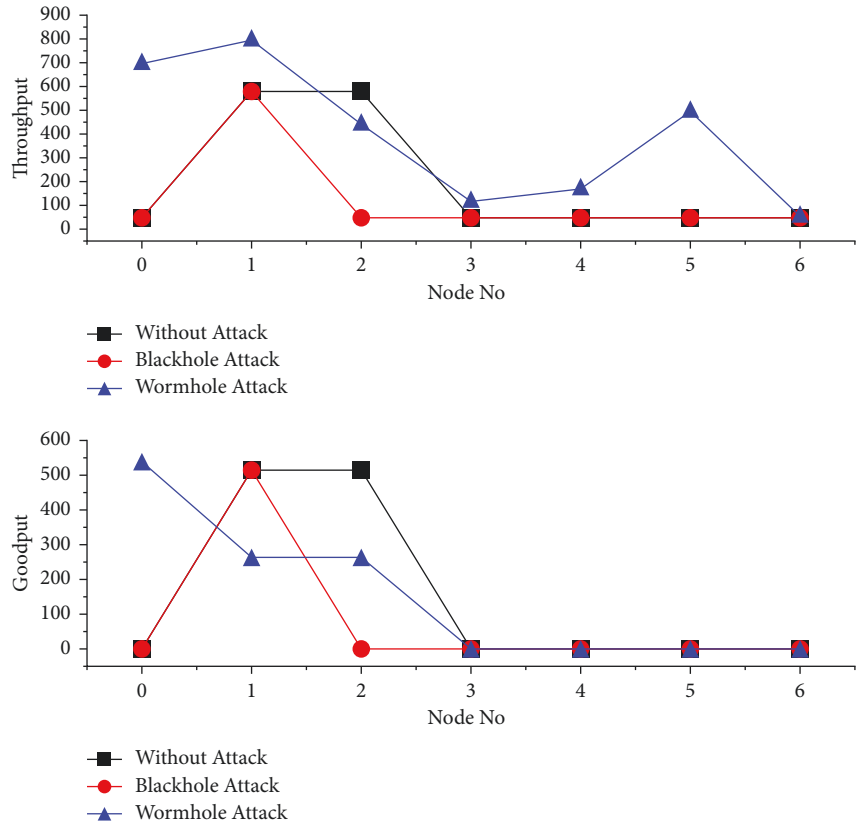


Figure 19: 7 MANET enabled IoT nodes.

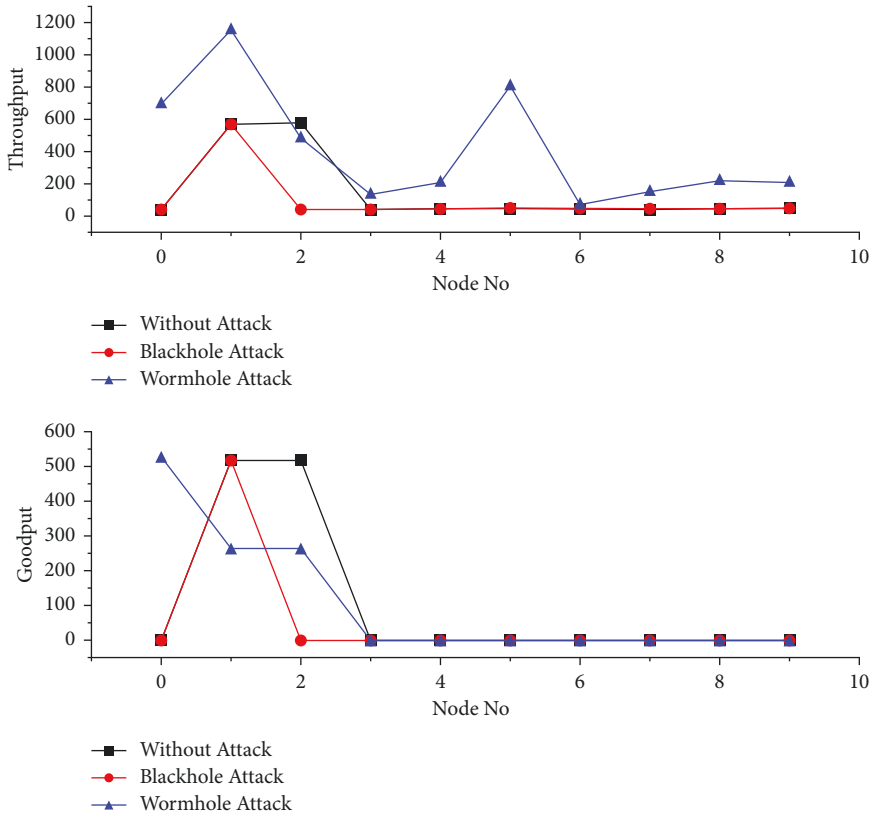


Figure 20: 10 MANET enabled IoT nodes.

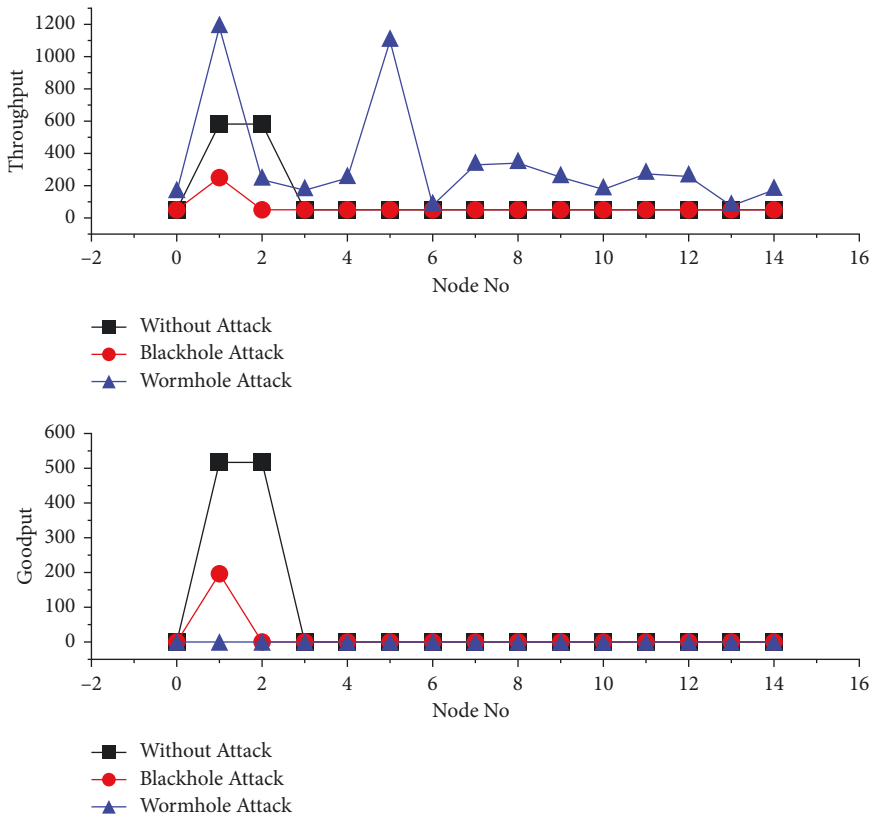


Figure 21: 15 MANET enabled IoT nodes.

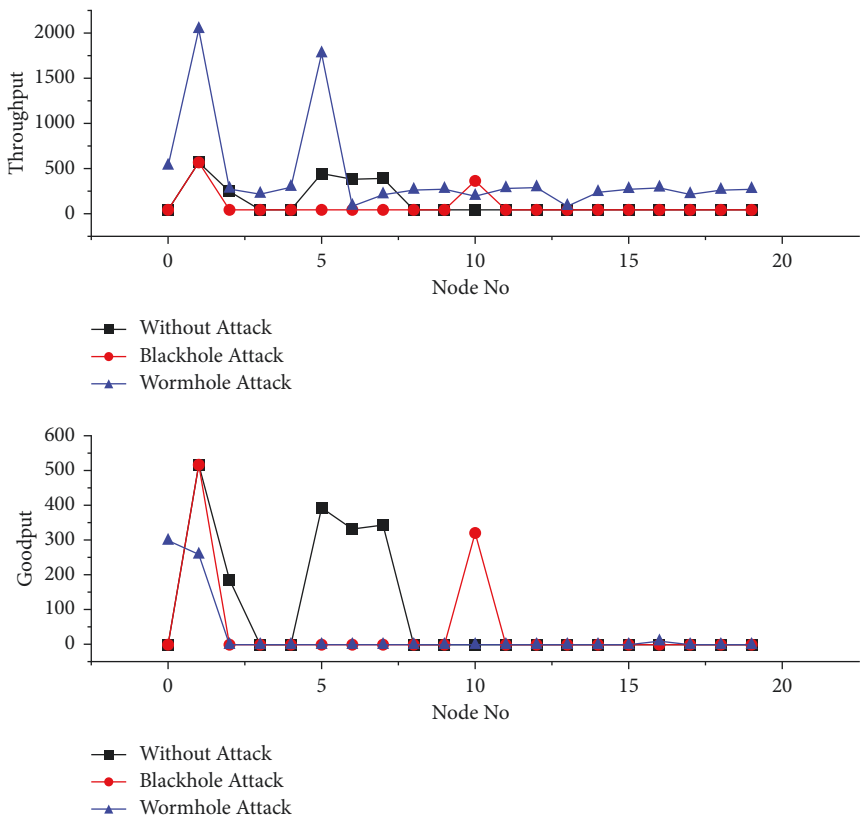


Figure 22: 20 MANET enabled IoT nodes.

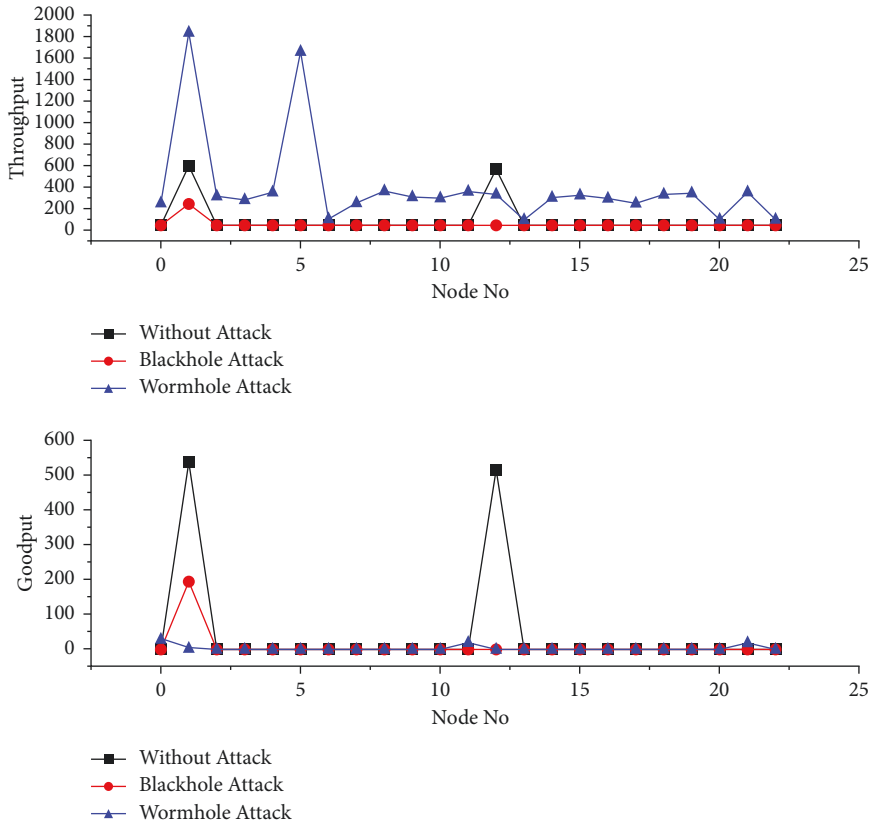


Figure 23: 23 MANET enabled IoT nodes.

cases, whereas the GP of wormhole attack is 0 across all IoT nodes within the cloud MANET enabled IoT network. Hence, it is clear that as the number of participating IoT nodes in cloud MANET enabled IOT network increases, the TP is higher with respect to the GP.

4.2.4. 20 Cloud MANET Enabled IoT Nodes. The TP and GP in Figure 22 illustrate that the same condition of IoT nodes performing normal operation (without attack) is higher than that of blackhole and wormhole attack. TP of IoT nodes under wormhole attack is better than that under the blackhole attack due to tunneling and data retransmission as well as protocol overhead.

4.2.5. 23 Cloud MANET Enabled IoT Nodes. The TP of wormhole attack is high on all IoT nodes as shown in Figure 23. However, the TP of IoT nodes is the same in the start in case of blackhole attack and decreases as soon as the number of nodes increases. The GP graph shows that the GP is very low of the overall cloud MANET enabled IoT network excluding on some IoT nodes. The throughput on every node is higher with respect to the GP because it includes data retransmission and protocol overhead. It is also observed that the TP of the overall cloud MANET enabled IoT network is higher in the presence of wormhole attack as compared to the blackhole attack when increasing the number of IoT nodes for monitoring. This is because of the tunneling availability of routing decisions in case of wormhole attacks.

5. Conclusions

The cyber security is a much concern when preserving the confidentiality, availability, and integrity of future networks. This concern even increases in Mobile Ad hoc Network (MANET) enabled Internet of Things (IoT) for varying and much personal IoT devices participating in communications. The application of MANET enabled IoT network in agricultural field towards making smart fields can talk and share its much important data and requires an independent network that serves as a cloud for many services such as monitoring in a secure and privately. Therefore, this paper compares the cloud-based services for MANET enabled IoT network under blackhole and wormhole attacks for IoT device-to-device information exchange. The agricultural field is simulated in a contextual view and simulated to observe the vulnerabilities towards Denial of Service (DoS) attacks such as blackhole and wormhole. The simulations are performed using an open-source simulator, Network Simulator 3 (NS-3), in order to determine the impact of blackhole and wormhole attacks on network performance of cloud MANET enabled IoT network deployed for monitoring of an agricultural field. The results are evaluated on the evaluations metrices such as throughput, packet delivery ratio (PDR), end-to-end delay (EED), and Jitter-Sum of preprocessed data gathered with the flow-monitor module of NS-3. This paper is highly useful for future cloud MANET enabled IoT smart agricultural field security research purpose.

Data Availability

Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Conflicts of Interest

The authors declare that they have no conflicts of interest to report regarding the present study.

Acknowledgments

This work was partly supported by the National Natural Science Foundation of China (Grant no. 62072060).

References

[1] W. S. Afifi, A. A. El-Moursy, M. Saad, S. M. Nassar, and H. M. El-Hennawy, "Importance of cloud computing in 5G radio access networks," *Research Anthology on Developing and Optimizing 5G Networks and the Impact on Society*, pp. 226–239, 2021.

[2] J. Huang, B. Lv, Y. Wu, Y. Chen, and X. Shen, "Dynamic admission control and resource allocation for mobile edge computing enabled small cell network," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 2, pp. 1964–1973, 2022.

[3] T. Alam, "Internet of things: a secure cloud-based MANET mobility model," *International Journal on Network Security*, vol. 22, no. 3, pp. 516–522, 2020.

[4] K. Yogeswaranathan and R. Collier, "A systematic survey on the role of cloud, fog, and edge computing combination in smart agriculture," *Sensors*, vol. 21, no. 17, Article ID 5922, 2021.

[5] Y. Chen, N. Zhang, Y. Zhang, X. Chen, W. Wu, and X. S. Shen, "TOFFEE: task offloading and frequency scaling for energy efficiency of mobile devices in mobile edge computing," *IEEE Transactions on Cloud Computing*, vol. 9, no. 4, pp. 1634–1644, 2021.

[6] Y. Chen, Y. Zhang, Y. Wu, L. Qi, X. Chen, and X. Shen, "Joint task scheduling and energy management for heterogeneous mobile edge computing with hybrid energy supply," *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8419–8429, 2020.

[7] J. Huang, C. Zhang, and J. Zhang, "A multi-queue approach of energy efficient task scheduling for sensor hubs," *Chinese Journal of Electronics*, vol. 29, no. 2, pp. 242–247, 2020.

[8] A. Aiiad, "An image hashing-based authentication and secure group communication scheme for IoT-enabled MANETs," *Future Internet*, vol. 13, no. 7, Article ID 166, 2021.

[9] K. Demestichas, N. Peppes, and T. Alexakis, "Survey on security threats in agricultural IoT and smart farming," *Sensors*, vol. 20, no. 22, Article ID 6458, 2020.

[10] C. Z. Sirmollo and M. A. Bitew, "Mobility-Aware routing algorithm for mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 6672297, 12 pages, 2021.

[11] S. Jaiganesh, K. Gunaseelan, and V. Ellappan, "IOT agriculture to improve food and farming technology," in *Proceedings of the Conference on Emerging Devices and Smart Systems (ICEDSS)*, pp. 260–266, Mallasamudram, India, March 2017.

[12] R. Trivedi and P. Khanpara, "Robust and secure routing protocols for MANET-based internet of things systems—a survey," emergence of cyber physical system and IoT in smart automation and robotics," *Advances in Science, Technology & Innovation (IEREK Interdisciplinary Series for Sustainable Development)*, Springer, Berlin, Germany, 2021.

[13] H. Gao, Y. Zhang, H. Miao, R. J. D. Barroso, and X. Yang, "SDTIOA: modeling the timed privacy requirements of IoT service composition: a user interaction perspective for automatic transformation from bpel to timed automata," *Mobile Networks and Applications*, vol. 26, 2021.

[14] X. Ma, H. Xu, H. Gao, and M. Bian, "Real-time multiple-workflow scheduling in cloud environments," *IEEE Transactions on Network and Service Management*, vol. 18, no. 4, pp. 4002–4018, 2021.

[15] Y. Huang, H. Xu, H. Gao, X. Ma, and W. Hussain, "SSUR: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center," *IEEE Transactions on Green Communications and Networking*, vol. 5, no. 2, pp. 670–681, 2021.

[16] Y. Yin, Z. Cao, Y. Xu, H. Gao, R. Li, and Z. Mai, "QoS prediction for service recommendation with features learning in mobile edge computing environment," *IEEE Transactions on Cognitive Communications and Networking*, vol. 6, no. 4, pp. 1136–1145, 2020.

[17] N. Papadakis, N. Koukoulas, I. Christakis, I. Stavrakas, and D. Kandris, "An IoT-based participatory antitheft system for public safety enhancement in smart cities," *Smart Cities*, vol. 4, no. 2, pp. 919–937, 2021.

[18] R. R. Chandan and P. K. Mishra, "Performance analysis of AODV under black hole attack," in *Proceedings of the 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*, March, 2019.

[19] H. Gao, X. Qin, R. J. D. Barroso, W. Hussain, Y. Xu, and Y. Yin, "Collaborative learning-based industrial IoT API recommendation for software-defined devices: the implicit knowledge discovery perspective," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 6, no. 1, pp. 66–76, 2022.

[20] G. Nagasubramanian, R. K. Sakthivel, and R. Patan, "Detection and isolation of black hole attack in mobile ad hoc networks: a review," *Disruptive Technologies in Information Sciences*, vol. 11419, Article ID 114190N, 2020.

[21] R. Rana and R. Kumar, "Performance analysis of AODV in presence of malicious node," *Acta Electronica Malaysia*, vol. 3, no. 1, pp. 1–5, 2019.

[22] P. Varga, S. Plosz, G. Soos, and C. Hegedus, "Security threats and issues in automation IoT," in *Proceedings of the IEEE 13th Int. Workshop FactoryCommun. Syst. (WFCS)*, pp. 1–6, Trondheim, Norway, May 2017.

[23] S. Palacharla, M. Chandan, K. Teja, and G. Varshitha, "Wormhole attack: a major security concern in internet of things (IoT)," *International Journal of Engineering and Technology*, vol. 7, no. 3, pp. 147–150, 2018.

[24] A. David, J. Gutiérrez, and S. Kumar Ray, "A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks," *Australian Journal of Telecommunications and the Digital Economy*, vol. 5, pp. 50–69, 2017.

[25] S. Murali and A. Jamalipour, "A lightweight intrusion detection for sybil attack under mobile RPL in the internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 379–388, 2020.

[26] J. Karlsson, L. S. Dooley, and G. Pulkkis, "Secure routing for MANET connected Internet of Things systems," in *Proceedings of the IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 114–119, Barcelona, Spain, August 2018.

[27] M. G. Samarasinghe and K. A. Kulawansa, "Use of IOT for smart security management in agriculture," in *Proceedings of the 9th Intl. Conf. on Advances in Computing, Control and Networking*, London, UK, July 2019.

[28] S. Laxmi, B. Hemavati, and B. Biradar, "Design and implementation of IoT based smart security and monitoring for connected smart farming," *International Journal of Computer Application*, vol. 179, no. 11, 2018.

[29] R. Haribabu, T. Santhosh, R. Sethupathi, S. Veerakumar, and A. Abinash, "Multiple tasks of IOT based smart security a monitoring devices for agriculture," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 3, 2017.

[30] P. Gupta, P. Goel, P. Varshney, and N. Tyagi, "Reliability factor based AODV protocol: prevention of black hole attack in MANET," *Smart Innovations in Communication and Computational Sciences*, Springer, Singapore, 2019.

[31] I. Kaushik, N. Sharma, and N. Singh, "Intrusion detection and security system for blackhole attack," in *Proceedings of the 2nd International Conference on Signal Processing and Communication (ICSPC)*, pp. 320–324, Coimbatore, India, March 2019.

[32] V. Kumar, "A review on detection of black hole attack techniques in MANET," *International Journal of Advanced Research*, vol. 4, no. 3, 2018.

[33] M. Imran, F. A. Khan, T. Jamal, and M. H. Durad, "Analysis of detection features for wormhole attacks in MANETs," *Procedia Computer Science*, vol. 56, pp. 384–390, 2015.

[34] M. Chernyshev, Z. Baig, O. Bello, and S. Zeadally, "Internet of things (IoT): research, simulators, and testbeds," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 1637–1647, 2018.

[35] L. Campanile, M. Gribaudo, M. Iacono, F. Marulli, and M. Mastroianni, "Computer network simulation with ns-3: a systematic literature review," *Electronics*, vol. 9, no. 2, 2020.

[36] A. Hinds, M. Ngulube, S. Zhu, and H. Al-Aqrabi, "A review of routing protocols for mobile ad-hoc networks (manet)," *International journal of information and education technology*, vol. 3, no. 1, 2013.

[37] S. Gurung and S. Chauhan, "A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET," *Wireless Networks*, vol. 25, no. 4, pp. 1685–1695, 2019.

[38] C. Aydogdu and E. Karasan, "Goodput and throughput comparison of single-hop and multi-hop routing for IEEE 802.11 DCF-based wireless networks under hidden terminal existence," *Wireless Communications and Mobile Computing*, vol. 16, no. 9, pp. 1078–1094, 2016.