drones

*Article*

# A UAV-Assisted Stackelberg Game Model for Securing IoMT Healthcare Networks

**Jamshed Ali Shaikh [1], Chengliang Wang [1,*], Muhammad Asghar Khan [2], Syed Agha Hassnain Mohsan [3], Saif Ullah [4], Samia Allaoua Chelloug [5], Mohammed Saleh Ali Muthanna [6] and Ammar Muthanna [7]**

1 Department of Computer Science and Technology, College of Computer Science, Chongqing University, Chongqing 400044, China; jamshed@cqu.edu.cn
2 Department of Electrical Engineering, Hamdard Institute of Engineering &Technology, Hamdard University, Islamabad 44000, Pakistan; m.asghar@hamdard.edu.pk
3 Optical Communications Laboratory, Ocean College, Zhejiang University, Zheda Road 1, Zhoushan 316021, China; hassnainagha@zju.edu.cn
4 Department of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400044, China; l202010009@stu.cqupt.edu.cn
5 Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; sachelloug@pnu.edu.sa
6 Institute of Computer Technologies and Information Security, Southern Federal University, Taganrog 347922, Russia; muthanna@sfedu.ru
7 Department of Applied Probability and Informatics, RUDN University, 6 Miklukho-Maklaya St., Moscow 117198, Russia; muthanna.asa@spbgut.ru
* Correspondence: wangcl@cqu.edu.cn

**Abstract:** On the one hand, the Internet of Medical Things (IoMT) in healthcare systems has emerged as a promising technology to monitor patients' health and provide reliable medical services, especially in remote and underserved areas. On the other hand, in disaster scenarios, the loss of communication infrastructure can make it challenging to establish reliable communication and to provide timely first aid services. To address this challenge, unmanned aerial vehicles (UAVs) have been adopted to assist hospital centers in delivering medical care to hard-to-reach areas. Despite the potential of UAVs to improve medical services in emergency scenarios, their limited resources make their security critical. Therefore, developing secure and efficient communication protocols for IoMT networks using UAVs is a vital research area that can help ensure reliable and timely medical services. In this paper, we introduce a novel Stackelberg security-based game theory algorithm, named Stackelberg ad hoc on-demand distance vector (SBAODV), to detect and recover data affected by black hole attacks in IoMT networks using UAVs. Our proposed scheme utilizes the substantial Stackelberg equilibrium (SSE) to formulate strategies that protect the system against attacks. We evaluate the performance of our proposed SBAODV scheme and compare it with existing routing schemes. Our results demonstrate that our proposed scheme outperforms existing schemes regarding packet delivery ratio (PDR), networking load, throughput, detection ratio, and end-to-end delay. Specifically, our proposed SBAODV protocol achieves a PDR of 97%, throughput ranging from 77.7 kbps to 87.3 kbps, and up to 95% malicious detection rate at the highest number of nodes. Furthermore, our proposed SBADOV scheme offers significantly lower networking load (7% to 30%) and end-to-end delay (up to 30%) compared to existing routing schemes. These results demonstrate the efficiency and effectiveness of our proposed scheme in ensuring reliable and secure communication in IoMT emergency scenarios using UAVs.

**Keywords:** secure medical healthcare network; internet of things; unmanned aerial vehicles; stackelberg game theory; black hole attacker



**Citation:** Shaikh, J.A.; Wang, C.; Khan, M.A.; Mohsan, S.A.H.; Ullah, S.; Chelloug, S.A.; Muthanna, M.S.A.; Muthanna, A. A UAV-Assisted Stackelberg Game Model for Securing IoMT Healthcare Networks. *Drones* **2023**, *7*, 415. https://doi.org/10.3390/drones7070415

Academic Editor: Diego González-Aguilera

Received: 10 May 2023
Revised: 16 June 2023
Accepted: 20 June 2023
Published: 23 June 2023

## 1. Introduction

The Internet of Medical Things (IoMT) is a rapidly growing field representing an interconnected network of medical devices, software applications, and health systems [1]. The IoMT network of devices and applications enables healthcare providers to collect, store, and analyze patient data in real-time applications, facilitating the efficient diagnosis, treatment, and monitoring of patient's health [2]. However, with the increasing connectivity of medical devices and systems, concerns have also grown in areas where it is difficult to have proper infrastructure. This is where unmanned aerial vehicles (UAVs) use in the context of secure communication systems in IoMT emerges as a promising solution [3]. UAVs, commonly known as drones, have proven helpful in various fields, and their potential applications in the healthcare industry are vast owing to their compatibility [4]. One such application assists IoMT networks in offering reliable services everywhere. UAVs are employed in several ways to enhance the efficiency of IoMT systems, protect patient data, and ensure the integrity of medical devices. UAVs equipped with sensors and cameras are used to monitor the physical security of healthcare facilities and provide real-time video feed to security personnel [5]. UAVs also conduct aerial surveillance of large medical facilities, providing a bird's-eye view of the facility and its surroundings and detecting potential security breaches [6].

In addition, UAVs can monitor the security of medical devices and equipment. Medical devices are increasingly connected to the Internet, making them vulnerable to cyberattacks [7]. UAVs with sensors and software can detect unauthorized access to medical devices and prevent potential cyberattacks. Due to the compactable nature of UAVs, they are used for inspecting and maintaining the physical security of medical devices [8]. They can fly to hard-to-reach locations and check medical devices for tampering or damage [9]. UAVs have proven to be very efficient in quickly surveying the damage caused by a disaster, such as a natural disaster or a terrorist attack [10]. They can provide real-time video feeds of the affected areas, helping healthcare providers and security personnel better understand the situation and take appropriate action [11]. Another application is to transport medical supplies and equipment in disaster response situations, UAVs can fly over impassable terrain and deliver much-needed medical supplies to the affected areas quickly and efficiently [12]. In particular, UAVs transport medical personnel to disaster sites, enabling them to provide prompt medical assistance to affected individuals [13].

Along with the above applications, UAVs can improve IoMT system security. They can detect and mitigate cyber threats to IoMT systems, providing an additional security layer [14]. Furthermore, UAVs are deployed in government and sensitive areas. To monitor the physical security of data centers and other critical infrastructures, ensuring they are protected from physical threats, such as theft or vandalism. UAVs have immense potential in the context of security systems within the IoMT networks. These sensors can monitor hospitals, medical equipment, and other assets for physical safety [15]. UAVs can also detect and mitigate cyber threats to IoMT systems, ensuring patient data security and integrity. In disaster response situations, UAVs have proven efficient in surveying damage, transporting medical supplies and personnel, and providing real-time video feeds of the affected areas [16]. With the rapid development of UAV technology and its increasing affordability, UAVs are expected to play a vital role in the security of IoMT systems [17].

To the best of our knowledge, integrating the IoMT networks with UAVs holds great promise for improving healthcare delivery in remote and underserved areas [18]. However, this integration presents significant challenges, particularly in security and privacy. UAVs are vulnerable to attacks that can compromise user data and disrupt services [19]. Despite existing research on IoMT-UAV integration, little attention has been given to addressing these security concerns. Various types of attacks, such as denial of service attacks, man-in-the-middle attacks, and phishing attacks, can compromise the security and privacy of patient data. Previous research assumes various kinds of attacks are encountered before they harm any data or network resources. However, practically there exist hacker attacks that harm user data. In particular, there is no way to retrieve compromised user or UAV

data in the event of an attack. Therefore, we have introduced a Stackelberg game model based on IoMT networks to tackle this issue to guarantee data safety and recovery success. We have adopted pure and mixed strategies to encounter the black hole attacks.

Furthermore, our proposed scheme provokes the SEE technique to recover the resource in case it is hacked. Game theory [20] is a mathematical framework widely used to analyze strategic interactions between multiple decision-makers, where each decision's outcome depends on others' decisions [21,22]. In the context of UAVs, game theory is an efficient technique for modelling and analyzing the interactions between multiple UAVs, UAVs, and ground-based agents and between numerous ground-based agents coordinating with UAVs [23]. One application of game theory in UAVs is cooperative surveillance, in which multiple UAVs work together to monitor a target area. Using game theory, researchers can model the strategic interactions between UAVs and optimize their surveillance strategies to maximize coverage and minimize resources used. Another application is UAV routing and scheduling, where multiple UAVs need to coordinate their routes and schedules to reduce collision risks and maximize efficiency. Game theory can be used to model strategic interactions between UAVs and optimize their routes and schedules to achieve the best overall outcome [24]. Figure 1 presents a taxonomy that classifies attacks in IoMT UAV networks based on network, device, and physical attacks. The taxonomy is a valuable tool for identifying and mitigating potential security threats in IoMT UAV networks, which are crucial for providing reliable and timely medical services in emergencies. As IoMT and UAVs are increasingly adopted in healthcare systems, the security of communication and data exchange between these devices becomes paramount. Taxonomy in Figure 1 provides a systematic framework for analyzing and categorizing threats to IoMT UAV networks, enabling researchers and practitioners to develop effective security solutions that protect the privacy and integrity of patient data.

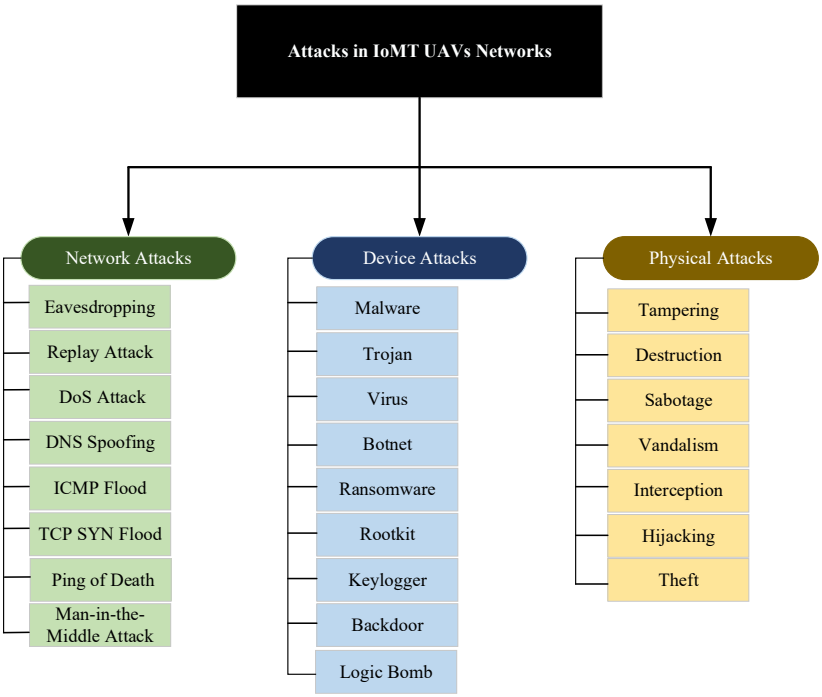


**Figure 1.** Taxonomy of IoMT.

### *1.1. Internet of Medical Things Assisted UAV Network Architecture and Challenges*

Figure 2 depicts a three-layer architecture for an IoMT-assisted UAV network consisting of the monitoring or doctor (DR) layer, the network layer, and the patients' layer. The DR layer monitors, collects, and stores data from various sources, including medical devices, sensors, and UAVs. This layer includes storage servers, data management

software, and security protocols to ensure data integrity and confidentiality. The network layer connects the devices and components of the system, encompassing communication protocols, routing algorithms, and network topology design to ensure reliable and efficient data transmission between devices in the patients' layer and the DR layer. The patient layer includes medical devices and sensors that directly interact with patients, such as wearable devices, monitoring equipment, and medical implants. The network layer sends patient data to the DR layer for medical analysis.

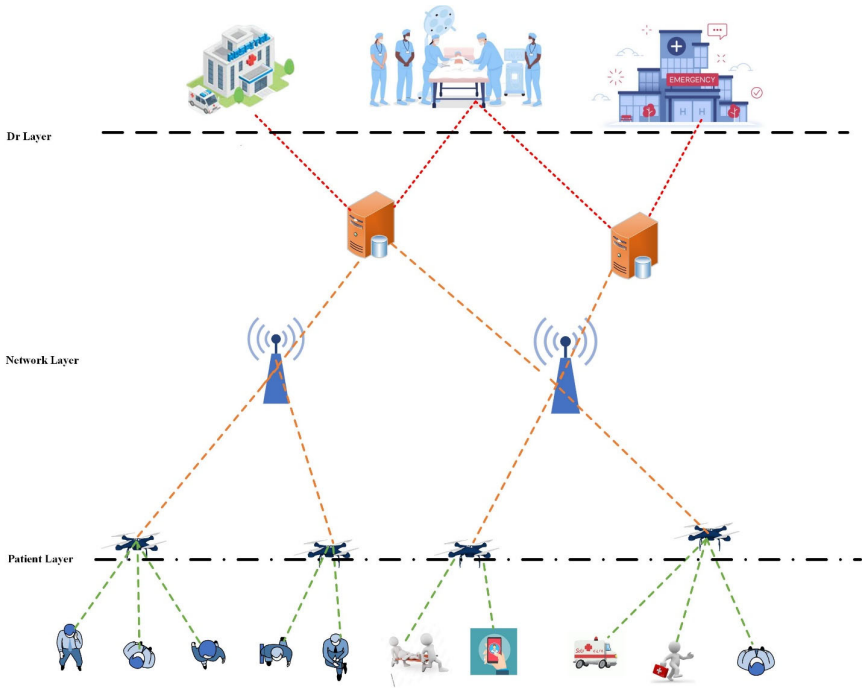


**Figure 2.** IoMT-assisted UAVs network architecture.

Using unmanned aerial vehicles (UAVs) in healthcare settings can impact patient privacy and data security in several ways. One of the main concerns is the potential for unauthorized access to sensitive patient information during data transmission between network-layer devices and patient-layer devices. Additionally, UAVs can be vulnerable to cyberattacks, data breaches, and unauthorized access by third parties, which can lead to the loss or theft of patient data. While using UAVs in healthcare settings can offer many benefits, mitigating the potential risks to patient privacy and data security is essential. By implementing strong security measures and policies, it is possible to ensure that UAVs can be used safely and effectively in healthcare environments while protecting patient privacy and data security. To address these concerns, one potential solution is using the Stackelberg game theory model. This model can provide a secure and efficient communication network for IoMT devices in healthcare settings. The model uses UAVs as an assistant for the IoMT devices, which can help to ensure secure data transmission. The model also incorporates a security mechanism using a lightweight Nash equilibrium to protect the data transmitted between the network and patient layer devices. This helps prevent unauthorized access to sensitive patient information and protects patients' privacy.

Despite the potential benefits of IoMT-assisted UAV network architecture, many challenges must be overcome to ensure the effective implementation of such a system. Protecting the security and confidentiality of sensitive medical data during transmission across networked devices is one of the most significant obstacles. This requires sophisticated security measures and encryption technologies to prevent unwanted access and data breaches. Integration and interoperability of many medical devices and sensors at the patient layer, which may employ multiple communication protocols or data formats, is

an additional issue. Ensuring compatibility and seamless integration of these devices is critical for accurate data collection and analysis.

Additionally, using UAVs in the network layer introduces challenges such as limited battery life, signal interference, and navigation in remote or difficult-to-access areas. Addressing these challenges will be critical for successfully deploying and operating IoMT-assisted UAV network architecture. To further enhance the security of this architecture, the proposed work can be used to implement secure routing and protect against potential rogue devices and malicious nodes. This approach can facilitate the secure transmission of sensitive medical data, ultimately improving the quality of care, quality of service (QoS), and patient health outcomes. For a better understanding of the terms used in this paper, we have described each abbreviation with its definition in Table 1.

**Table 1.** List of Abbreviations.

| Abbreviations | Definitions |
|---|---|
| IoT | Internet of things |
| IoMT | Internet of Medical Things |
| UAVs | Unmanned aerial vehicles |
| AODV | Ad hoc on-demand distance vector |
| SBAODV | Stackelberg ad hoc on-demand distance vector |
| DR | Doctor layer |
| MAC | Media access control |
| UDP | User datagram protocol |
| TCP | Transmission control protocol |
| HTTP | Hypertext transfer protocol |
| NRL | Network routing load |
| SSE | Strong Stackelberg equilibrium |
| PDR | Packet delivery ratio |
| QOS | Quality of service |
| RREQ | Route-request |
| RREP | Route reply |
| FRREP | Fake route reply |
| NS2 | Network simulator two |
| MANETs | Mobile ad hoc networks |
| LPNRP | Low-power and noisy routing protocol |
| TPH | Tree protocol for healthcare |
| RPH | Routing protocol for healthcare |
| FDTRP | Fuzzy dynamic trust-based routing protocol |
| DADRP | Dual attack detection routing protocol |
| CBR | Constant bit rate |

### *1.2. Proposed Scheme and Contributions*

In this study, we adopted the Stackelberg game theory model, in which we consider a black hole an attacker and a UAV a defender. The proposed scheme considers two scenarios: first, where attackers try to attack all resources of the UAV, and the attacker tries to find weak resources by using a probability function. To address these issues, we proposed the Stackelberg ad hoc on-demand distance vector (SBAODV) scheme, which offers the best solution to overcome these challenges. In the below table, we have mentioned benchmark routing schemes for UAVs in the IoMT network.

In summary, the main contributions of this paper are as follows:

- Our proposed method can detect malicious devices that attack IoMTs. Specifically, UAVs are more vulnerable to attackers due to a lack of advanced algorithms.
- We introduced the Stackelberg game theory model to allow healthcare networks to identify potential security threats before they occur. In case the data are affected, defenders can take proactive measures to secure their networks, prevent attacks, and recover the data.

- The proposed scheme allows healthcare networks to quickly adapt to changing security threats. By constantly monitoring the network and modeling the interactions between attackers and defenders, healthcare networks can adjust their security measures to respond to new threats as they arise.

This paper is organized as follows: Section 2 summarizes related work. Section 3 describes our approach to securing the IoMT network. Further, this section details the algorithm and its implementation. Section 4 describes the simulation and experimental setup to compare our suggested approach to the current algorithm. The analytical results and implications are presented here. Section 5 reviews the paper's key findings and discusses further research. This paper concludes with its references.

## 2. Related Works

Many authors have proposed various models to address the security and privacy issues in healthcare systems based on UAVs. UAVs are gaining popularity in various domains, including healthcare. In healthcare, UAVs are used for emergency medical transportation, assisting patients in remote areas, and delivering essential medical supplies [25]. This paper presents a detailed review of related work on using UAVs in emergency medical situations, focusing on healthcare networking. Moreover, we discuss current leading-edge technologies and their limitations in this field.

The authors [26] presented an overview of current technologies related to medical healthcare systems and discussed their advantages and limitations. The authors also proposed a framework for using UAVs in disaster relief situations. A comprehensive review of UAV-based emergency healthcare systems was presented. The authors discuss the challenges in healthcare systems during emergencies and how UAVs can be used to overcome these challenges [27]. The authors also described the various kinds of UAVs used in healthcare and their applications. The authors summarize the obstacles and prospects connected with UAV-assisted emergency healthcare networking [28]. The authors mentioned the adoption of UAVs in healthcare networks, with practical applications, and the limitations of current technologies. The authors also proposed a framework for using UAVs in emergency healthcare networks under disaster scenarios [29].

A systematic review of UAV-assisted healthcare services is provided in disaster management to rescue patients and offer a reliable integrated system by utilizing UAVs in IoMT networks. The authors also described the different disaster management stages and how UAVs can be used in each stage [30]. Developed an outdoor healthcare system for older people during emergencies, in which they adopted UAVs and the Internet of Things IoT devices. The proposed scheme provides real-time assistance to older adults during emergencies and forwards emergency information through communication networks. On the other hand, computer-assisted treatment was defined in [31] as a psychotherapeutic or behavioral treatment given over an IoMT network. This method is becoming more popular as a quick and cheap way to help people with mental health problems who may have trouble getting to traditional therapies.

There is a growing trend toward providing care outside the hospital for extended periods, and constant supervision is essential. This is due to the high cost of hospitalization, which has led many countries to shift their health policies from reactive acute treatment to proactive care. The proposed schemes mainly focus on resource allocation and data delivery; unfortunately, none investigate security issues. Usually, the existence of black hole attackers tries to hack the data or produce fake data in order to breach other users' privacy. To tackle these issues, the proposed IoMT-assisted treatment, the Stackelberg game theory algorithm, aims to protect IoMT medical healthcare networks from black hole attackers and is an approach in which game theory is used to develop an algorithm. A black hole attacker is a malicious entity that intercepts and redirects network traffic to a black hole, effectively disrupting network communication. The Stackelberg game theory algorithm involves two players the victim or defender (healthcare provider) and the attacker user (black hole attacker). The defender aims to protect the network from the attacker, while the attacker aims to intercept and redirect network traffic. Base on

above literature view we have formed table of comparison which shows the advantages and drawbacks of privacy security issues of some famous schemes in medical healthcare networking indicated in Table 2.

**Table 2.** Related work with their advantages and drawbacks of privacy security issues of medical healthcare networking assisted UAV in emergency scenarios.

| References | Technique | Advantages | Drawbacks |
|---|---|---|---|
| [32] | UAV-assisted wireless networks for emergency healthcare | Fast deployment, easily accessible in remote areas, real-time monitoring | Limited payload capacity, potential privacy breaches |
| [33] | Privacy-preserving medical data sharing in UAV-assisted healthcare networks | Data encryption, secure data sharing among healthcare providers | Increased data storage and processing requirements |
| [34] | Multi-UAV cooperation in medical emergency scenarios | Efficient resource allocation, improved coverage | Complex cooperation mechanisms, scalability issues |
| [35] | Securing UAV-assisted healthcare networks with blockchain | Decentralized data management, enhanced security | High energy consumption, and scalability concerns |
| [36] | Artificial intelligence-based anomaly detection in UAV-assisted healthcare networks | Real-time threat detection, improved network security | False positives, privacy issues |

## 3. System Model

The system model introduced in this paper aims to address the security issue in UAV-based IoMT networks. The model consists of three key sub-sections. In the first subsection, we explore the characteristics of black hole UAVs, which maliciously drop data packets. In the second subsection, we propose a Stackelberg game theory-based scheme to mitigate the impact of attackers in the network, including black hole UAVs. Finally, in the third subsection, we present a pseudo-code algorithm for data protection that can be implemented in the network to safeguard against potential attacks. These sub-sections provide a comprehensive solution for securing UAV-based IoMT networks against attacks, including those from black hole UAVs.

### *3.1. Understanding the Characteristics of Black Hole UAVs*

Drone routing protocols are designed for networks of UAV00s and are typically based on ad hoc networking principles. Ad hoc networks are characterized by their decentralized nature, where UAVs can transfer data with each other directly without any centralized infrastructure. Drone networks are often used for aerial surveillance, search and rescue, and package delivery applications. In an ad hoc UAV network, each UAV preserves a routing table that contains information about its neighbors and the routes to other nodes in the network. When a UAV wants to forward data packets to the destination node, it initially checks its routing table to search for a direct route to the destination. If there is no route in the routing table, the UAV broadcasts a route request (RREQ) packet to its neighbors. Usually, the RREQ packet contains information about the source and destination nodes and a sequence number to prevent loops. However, a black hole UAV can disrupt communication and cause significant damage to the network. A black hole UAV is a malicious node that drops or selectively forwards packets to false routs instead of delivering them to their destination.

The black hole UAV can introduce a fake reply in the network by sending fake route reply (FRREP) packets with itself as the next hop for a given destination. This can lead to the loss or compromise of sensitive data. The black hole UAV can exploit vulnerabilities in the routing protocol used in the UAV ad hoc network, such as the lack of authentication in RREQ and RREP packets. Figure 3 presents the flow of packets in an ad hoc UAV network in the presence of a black hole UAV. UAV-A is the source node that wants to send data to UAV-F, the destination UAV. UAV-E is the black hole UAV that drops all packets it receives. The other UAVs, UAV-B, UAV-C, and UAV-D are intermediate UAVs that forward

packets toward their intended destination. If the packets are routed through UAV-E, they will be dropped and not reach their intended destination. This can cause communication disruptions and lead to losing or compromising sensitive data.

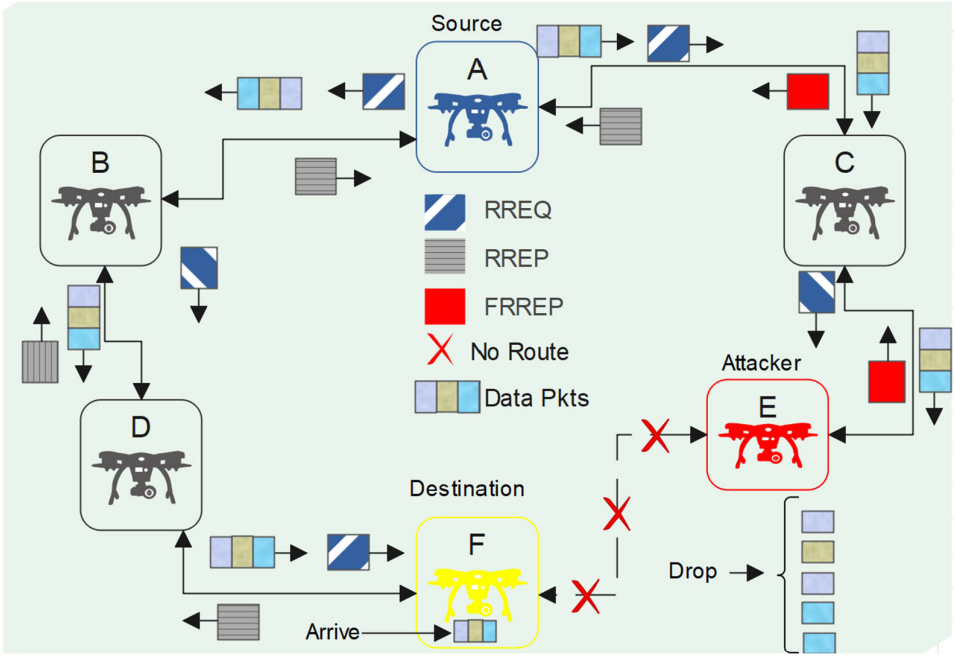


**Figure 3.** Routing strategy with a black hole in UAV network scenario.

Table 3 presents a comprehensive view of the routing table for an ad hoc UAV network, explicitly highlighting the path packets take from UAV-A to UAV-F. The routing tables for UAV-A, F, and E have been merged to provide a global perspective on the network topology. The table lists all the destinations in the network and their corresponding next-hop nodes and metrics, providing a complete picture of the routing paths in the network. Furthermore, the table shows the route discovery process for each destination, including the RREQ and RREP packets sent and received by each node. This information can be used to trace the path taken by packets and identify any potential bottlenecks or vulnerabilities in the network. The "Fake-E" column in the table is exciting, indicating whether the RREP packet received from UAV-E is genuine or fake. This information is crucial for detecting and avoiding compromised routes, which can lead to the loss or compromise of sensitive data. Overall, this routing table provides valuable insights into the topology and functioning of the ad hoc UAV network. It can be used as a reference for optimizing network performance and enhancing security.

**Table 3.** Global routing table for UAV ad hoc network (A, E, F).

| Destination | Next Hop | Metric | RREQ-A | RREP-A | RREQ-F | RREP-F | Fake-E |
|---|---|---|---|---|---|---|---|
| UAV-A | - | 0 | - | - | Yes | Yes | No |
| UAV-B | UAV-D | 2 | No | Yes | No | Yes | Yes |
| UAV-C | UAV-B | 2 | No | Yes | No | Yes | Yes |
| UAV-D | UAV-F | 2 | No | Yes | No | Yes | Yes |
| UAV-E | - | 0 | Yes | Yes | Yes | Yes | No |
| UAV-F | - | 0 | Yes | Yes | - | - | No |

### *3.2. Proposed Stackelberg Security-Based Game Theory Algorithm for Securing IoMT Networks Using UAVs*

This subsection presents our proposed Stackelberg security-based game theory algorithm for securing IoMT networks using UAVs. Our algorithm is designed to detect and

recover data affected by black hole attacks, a common type of attack in IoMT networks. The Stackelberg game theory model is a powerful tool for analyzing decision-making when multiple parties have conflicting interests. In our proposed scheme, the UAV network is modeled as a game competition between the attacker, who aims to disrupt communication, and the defender, who aims to protect the network. We utilize the strong Stackelberg equilibrium (SSE) to formulate strategies that protect the system against attacks. Our proposed algorithm consists of two main components: the Stackelberg game theory scheme and the critical features of the UAV-assisted Stackelberg game model. In the following sections, we describe each component in detail.

3.2.1. Stackelberg Game Theory Scheme

The proposed scheme is based medical healthcare system where the information of each user is confidential; therefore, it is necessary to ensure the data's safety. Initially, we have considered 3D coordinates for the coverage area of UAVs. We have utilized the Euclidean distance formula for 3D coordinates in Equation (1) to calculate the distance between the UAV and end devices.

$$D = \sqrt{\left(x^2{}_{UAV} - x^2{}_{IoT}\right) + \quad \left(y^2{}_{UAV} - y^2{}_{IoT}\right) + \quad \left(z^2{}_{UAV} - z^2{}_{IoT}\right)} \tag{1}$$

where $D$ is the distance between $UAV$ and IoMT device, and $x$, $y$ and $z$ are their coordinates. After finding the distance, we have introduced a game theory model which plays a vital role in many research areas, particularly for the security and safety of wireless networks. We have utilized the Stackelberg game theory model for IoMT medical healthcare networks by considering special features of game theory. The proposed scheme consists of three main parts. (1). The number of resources $R = \{r_1, r_2, r_3, \ldots r_n\}$. (2). The set strategies $S = \{s1, s2, s3, \ldots\ldots sn\}$. (3) Utility functions $U = \{u1, u2, u3, \ldots\ldots un\}$.

In wireless networks, each user is considered a player; in this scenario, we have considered the Stackelberg game theory model for security purposes. This model described the competition between two users: attacker (leader) and defender (follower). Initially, the attacker may choose a target from Equation (2) where $T$ is a set of targets ($T$).

$$T = \{r1, r2, r3, \ldots\ldots rn\} \tag{2}$$

The victim or defender (UAV) will defend its resource from the attacker node; the set of victim resources ($Rs$) is described in Equation (3):

$$Rs = \{r1, r2, r3, \ldots\ldots rn\} \tag{3}$$

Assume a target $t_i$ is attacked and recovered; in this case, the defender's utility function is $U_d^c(t_i)$ (as mentioned in Equation (4). If it is not recovered $U_d^u(t_i)$ whereas the attacker's utility function $U_d^c(t_i)$ is greater in this case the utility value will be negative for the victim side as indicated in Equation (5).

$$U_d^c(t_i) - U_d^u(t_i) \; > \; 0 \tag{4}$$

$$U_d^u(t_i) - U_d^c(t_i) \; > \; 0 \tag{5}$$

From Equation (3), we can observe that if the target is recovered, the victim's or defender's utility function is positive. In case the attacker successfully hacks the data, the utility function of a victim is negative, as shown in Equation (4).

Usually, in security applications, the attacker's pure strategy is based on a set of specific targets. In contrast, in the case of a mixed strategy, the attacker's strategy is based on the probability of attacking targets as vectors A= [a_1, a_2,. . . . . a_n]. The victim's pure strategy is to protect the targets of vector ∈ {0,1} n. Let us assume that D ∈ {0,1} n the set of possible coverage vectors, and $m$ the vector of coverage probabilities. The defender contains

the set of the mixed strategies $M$ is defined as the vector of probabilities of choosing each $d \in$ D. For strategy $M$, the defender's utility is defined in Equation (6):

$$U_d(M,a) = \sum_{i=1}^{n} a_i(p_i U_d^m(t_i) + (1-m_i)U_d^u(t_i)) \quad (6)$$

The attacker's utility function based on mixed strategy where the attacker targets the particular resource from the set of coverage probabilities can be calculated from Equation (7).

$$U_a(M,a) = \sum_{i=1}^{n} a_i(m_i U_d^m(t_i) + (1-m_i)U_d^u(t_i)) \quad (7)$$

The Nash equilibrium may be calculated in games using symmetric security. In these instances, the defender will choose a strategy ($M$) that maximizes their utility above any alternative strategy ($M'$) available in Equation (8).

$$U_d(M,a) > U_d(M',a) \quad (8)$$

In the above equation $U_d(M,a)$ is the best strategy from all possible strategies and hence offers higher utility value. Similarly, the attacker will choose a strategy ($a$) that maximizes their utility over any alternative approach ($a'$) available to them as Equation (9) indicates.

$$U_d(M,a) > U_d(M,a') \quad (9)$$

In the Stackelberg security game, the victim or defender UAV decides first, and the attacker node chooses its strategy based on the defender's action. The function g($M$) = a represents the attacker's response to the defender's choice. The strong Stackelberg equilibrium (SSE) can be formulated by analyzing the game in this manner. Based on SSE the defender will make its best response strategy can be calculated in Equation (10).

$$U_d(M,g(M)) \geq (M',g(M')) \quad (10)$$

Here $U_d(M,g(M))$ is the best response strategy for all $M'$; moreover, attackers best response strategy would be

$$U_a(M,g(M)) \geq U_a(M',g'(M)) \quad (11)$$

Here Equation (11) shows the best response of the attacker. In our scenario, the victim or defender will choose its best response from the set of strategies to recover its target as Equation (12) presents.

$$U_d(M,g(M)) \geq U_d(M',\tau(M')) \quad (12)$$

We can observe in Figure 4a IoMT system based on UAV ad hoc networks where UAVs operate as an intermediate relay to forward data between a data center and end users. UAVs are adopted to provide efficient and secure data delivery; though they have limited resources and advanced algorithms, they are hot spots, black hole attackers. In Figure 4b, a black hole attacker finds and attacks UAV, damages the user's data, and destroys the network. In Figure 4c, we can see that when a black hole attacker tries to access the UAV's data, the victim UAV tries to respond with the help of a game-theoretic algorithm that defends itself to ensure users' security. The Stackelberg game theory ensures that in both cases when a black hole attacker tries to attack whole resources or find some weak spots, it succeeds. Furthermore, if a black hole attacker attacks data, the game theory utilizes its optimal strategy to recover the data. Finally, the defender UAV blocklists the attacker and informs all end devices about the attacker, making sure other users share any information with the black hole attacker by giving a black flag to it; on the other hand, the cooperative users have a white flag that describes the behavior of users in the network.

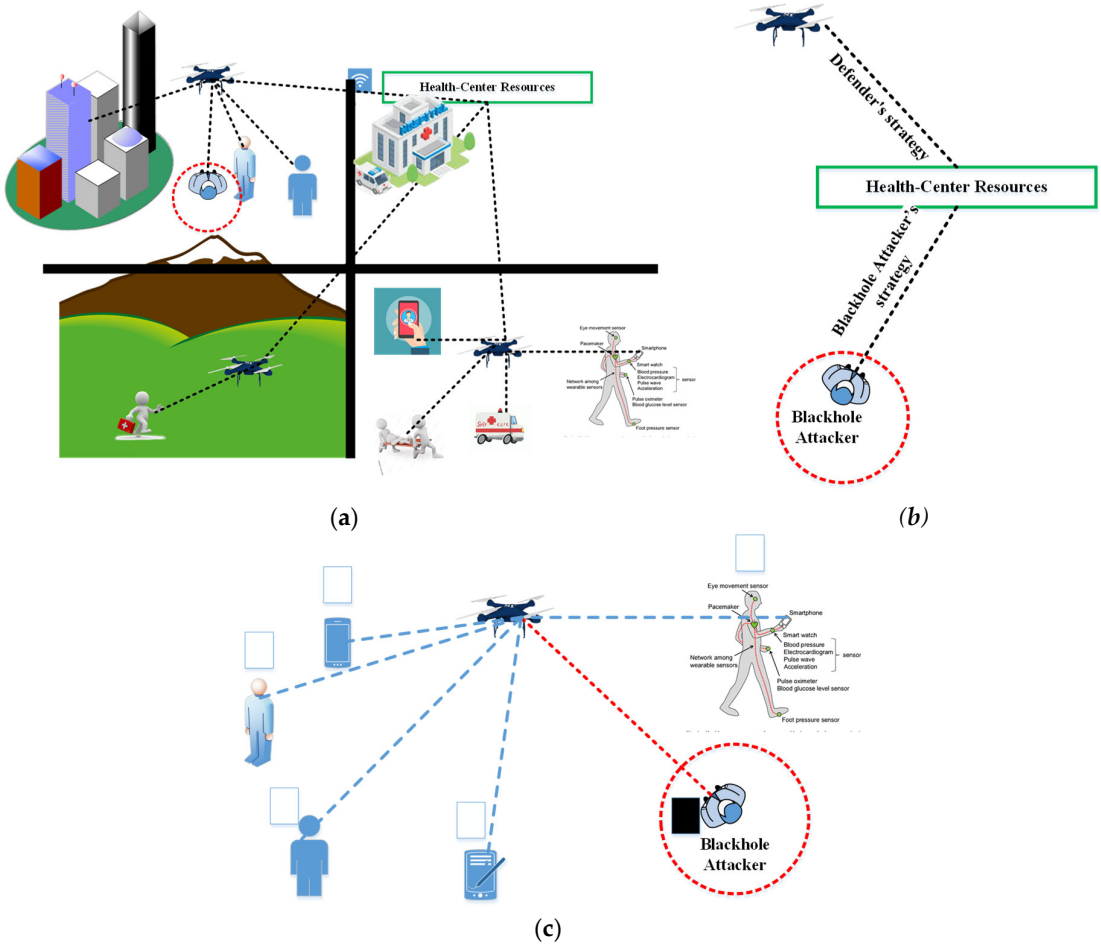


**Figure 4.** Working principle of medical healthcare networking assisted UAV in emergency scenarios. Figure(**a**) UAV assisted IoMT network, Figure(**b**) black hole attack and game theoretic strategies of defender and attacker and Figure (**c**) UAV defends its resources and block the black hole attacker.

#### 3.2.2. Key Features of the UAV-Assisted Stackelberg Game Model

The key features of the UAV-assisted Stackelberg game model for securing IoMT healthcare networks are its ability to provide a secure and efficient communication network. One of the main contributions of the model is its use of a Stackelberg game framework to model to secure the UAVs and the IoMT devices' data. This allows the attacker (black hole) or rogue medical device to act as a leader in the game, making strategic decisions to harm the UAV and hack the data. In response, the UAV acts as a defender to secure its data and form its strategies by utilizing the Stackelberg game theory model. This can help improve the accuracy and timeliness of healthcare data, leading to better patient diagnosis and treatment outcomes. Additionally, the model's use of moveable UAVs as assistants between network layer to patient layer devices can help overcome challenges associated with traditional fixed networks, such as limited coverage and interference from other wireless devices.

### *3.3. Algorithm Pseudo Code*

The proposed Algorithm 1 begins by initializing a network of N number of IoMT devices. The attacker selects a target resource to steal data from a victim IoMT device, as described in line 3. If the defender detects the attack, it responds by using a Stackelberg game strategy to protect its data, as seen in line 6. Both the attacker and defender use their best strategies. If the defender's utility value is higher than the attacker's expected utility value, the attacker cannot successfully hack the data, and the defender's data remains

protected. However, if the attacker's expected utility is higher, as described in lines 7 to 15 of the pseudocode, the attacker successfully hacks the data. However, the defender can recover it using the Stackelberg game theory. The game continues until either the attacker succeeds in hacking all available data or the defender successfully protects its data. The algorithm repeats these steps until all data are recovered. The algorithm's time complexity is O(N), where N is the network's total number of IoMT devices.

**Algorithm 1.** Pseudo code of secure ST game

**Input:** N: The total number of IoMT devices in the network.
**Output:** The data on the victim node remains protected.

```
1.  Initialize network with N devices
2.  Do
3.  {
4.      Attacker_node = select_attacker_node()
5.      Victim_node = select_victim_node(attacker_node)
6.      Defender_node = select_defender_node(victim_node)
7.      Utility_defender = calculate_defender_utility(defender_node)
8.      Utility_attacker = calculate_attacker_utility(attacker_node, victim_node)
9.      if (utility_defender > utility_attacker)
10.      {
11.          Protected_data = data_on_victim_node
12.      }
13.      Else
14.      {
15.          Hacked_data = data_on_victim_node
16.          Defender_node.update_strategy()
17.          Defender_node.recover_data()
18.      }
19.  } while (not all_data_protected());
```

Our proposed scheme leverages the power of game theory to detect and prevent attacks in real time, enabling timely responses to security threats. In contrast, existing techniques rely on traditional routing protocols that do not provide sufficient protection against black hole attacks in IoMT networks using UAVs. In the following Section 4, we provide a more detailed comparison of our proposed method with other related techniques and discuss the effectiveness of our work in securing communication in IoMT UAV networks.

## 4. Simulation Setup and Experimental Results

This section is divided into three parts. The first part briefly describes the network simulator tool used in the simulation. The second part describes the simulation parameters and environment, including the network topology, protocol, and introduction of a rogue device to disturb the network. In the third part, we present the results of the experimental work, including the evaluation of the proposed SBAODV scheme and a comparison with other routing protocols.

### *4.1. Network Simulator Two*

Network simulator two (NS2) [37] is an open-source network simulation software commonly used by researchers to evaluate the performance of different networking protocols and architectures. With a wide range of networking models and components, NS2 enables researchers to simulate various network topologies and conditions, allowing them to optimize their protocols and architectures. The simulation setup in NS2 involves defining the network topology, configuring network components, and specifying simulation parameters. NS2 supports the simulation of various network technologies, including wired and wireless networks, satellite networks, mobile ad hoc networks (MANETs), and sensor networks. Additionally, NS2 provides a range of protocols, such as transmission control

protocol (TCP), user datagram protocol (UDP), and hypertext transfer protocol (HTTP). Researchers use NS2 to simulate different network scenarios and evaluate the performance of their protocols and architectures under different network conditions [38]. The software also offers data visualization and analysis tools, enabling researchers to study the impact of different network configurations on protocol performance.

### *4.2. Experimental Setup*

For the validation of our proposed SBAODV routing protocol, we conducted simulations in NS2. As part of our work, we modified the ad hoc on-demand distance vector (AODV) routing protocol. We updated it with the proposed Stackelberg game theory scheme, resulting in the SBAODV routing protocol for hybrid IoMT network simulations. We designed a hybrid network topology for an IoMT scenario, assuming six fixed medical servers at different locations connected with wired topology and 110 wireless nodes, including UAVs, black holes, access points, medical nodes, and mobile nodes. During the experiment, we introduced a rogue device, also known as a black hole attacker, to disturb the network. The simulation area was set to 125 × 125 × 50 ($m^3$), and 110 nodes were randomly distributed within this area using a uniform random distribution policy, as commonly performed in the literature [38]. Although other distribution policies could have been considered for network topology development, we chose to use a uniform random distribution policy as a simple baseline for evaluating the performance of the IoMT network. We utilized the IEEE 802.15.4 Media access control (MAC) protocol, a low data rate wireless personal area network standard widely used in various low-power, low data rate, and low-cost communication applications [39,40].

To evaluate the efficiency of our proposed SBAODV scheme, we compared it with several other routing protocols, including low-power and noisy routing protocol (LPNRP) [32], tree protocol for healthcare (TPH) [41], a routing protocol for healthcare (RPH) [42], fuzzy dynamic trust-based routing protocol (FDTRP) [43], and dual attack detection routing protocol (DADRP) [44]. We assumed a reactive gateway as the IoMT gateway in the network and simulated the network for 600 s using a constant bit rate (CBR) traffic model and UDP application. Quality of service was evaluated based on several parameters, including average delay, jitter, packet deliver ratio % (PDR%), network routing load% (NRL%), throughput (kbps), and detection ratio %. A Drop Tail–Priqueue was used as the queue type. These parameters are summarized in Table 4, and the network environment is depicted in Figure 5.

**Table 4.** Simulation parameters.

| Parameters | Values |
|---|---|
| Number of nodes | 110 |
| Simulation area (3D) | 125 × 125× 50 ($m^3$) |
| Node placement | Uniform random distribution |
| Transmission range | 100 m |
| MAC protocol | IEEE 802.11.15.4 |
| Routing protocols | SBAODV, LPNRP, TPH, RPH, FDTRP & DADRP |
| Rouge device | As a black hole attacker |
| IoMT gateway node | Reactive gateway |
| Fixed medical server Nodes | 6 |
| Data rate | 100 Kb |
| Packet size | 512 Bytes |
| Simulation time | 600 s |
| Traffic model | CBR with UDP application |
| QoS | PDR%, NRL%, throughput (kbps), detection ratio %, end-to-end delay (ms), |
| Queue type | Drop Tail–Priqueue |

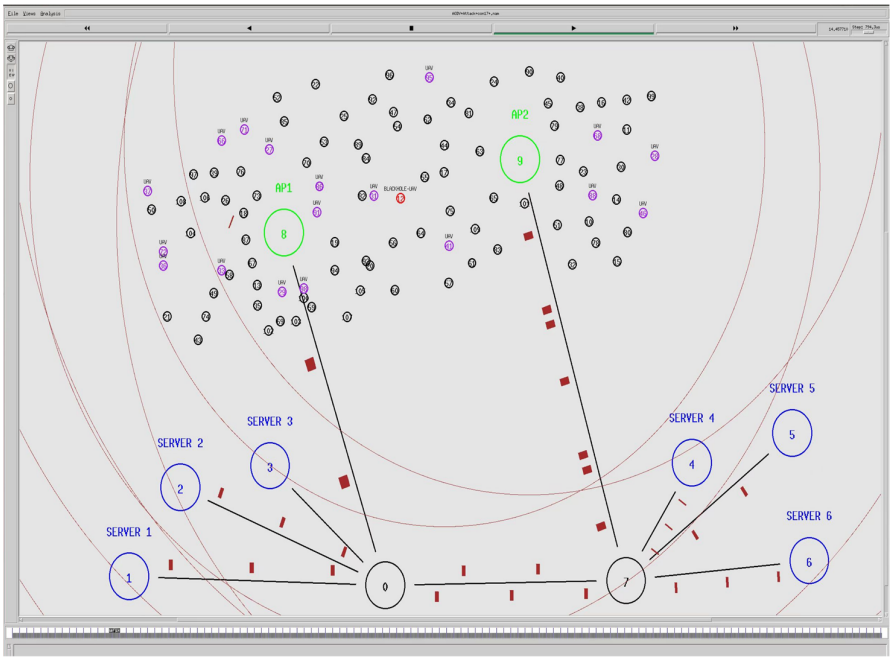


**Figure 5.** Experimental scenario in NS2 environment.

### *4.3. Analysis of Results*

This subsection presents an analysis of the performance of the proposed routing protocol in an IoMT network scenario. The analysis includes four key quality of service (QoS) parameters (a) packet delivery ratio (PDR%) is a quality of service (QoS) metric used to evaluate the reliability of a routing protocol. It measures the percentage of packets that are successfully delivered to their intended destination out of the total number of packets sent. In other words, it represents the ratio of the number of received data packets that reach their destination to the number of generated data packets sent. (b) Network routing load % (NRL%) measures the amount of routing overhead generated by the routing protocol, typically measured as the ratio of the number of routing packets generated to the number of data packets delivered in the network. (c) Throughput is a quality of service (QoS) metric used to evaluate the amount of data transmitted over a network in a given time period. It represents the rate at which data are successfully transmitted from the source to the destination, typically measured in kilobits per second (kbps) or megabits per second (Mbps). (d) Detection ratio (%) is a network security metric used to evaluate the effectiveness of a security system in detecting and preventing attacks. It measures the percentage of detected attacks out of the total number of attacks attempted on the network. In the following analysis, we present the results of each QoS parameter, along with their implications for the performance of the routing protocol in the IoMT network scenario.

#### 4.3.1. Packet Delivery Ratio (%) vs. No of Nodes

Figure 6 shows the packet delivery rate (PDR%) results of different routing protocols in IoMT-assisted UAV networks with varying numbers of nodes (20, 40, 60, 80, and 100). The protocols tested include LPNRP, TPH, RPH, FDTRP, DADRP, and SBAODV. The PDR% was evaluated as the ratio of the total number of successfully delivered packets divided by the total number of packets sent. At the 20-node number, the SBAODV protocol achieved a PDR% of 97%, significantly higher than the other protocols, with DADRP being the closest with a PDR% of 92%. As the number of nodes increases, the performance of all protocols tends to decrease. However, the SBAODV protocol maintains its superiority, achieving a PDR% of 94.29% on 40 nodes, 91.99% on 60 nodes, 89% on 80 nodes, and 86% on 100 nodes. This can be attributed to its ability to adapt to network topology changes and dynamically select the best path to the destination based on the available network resources.

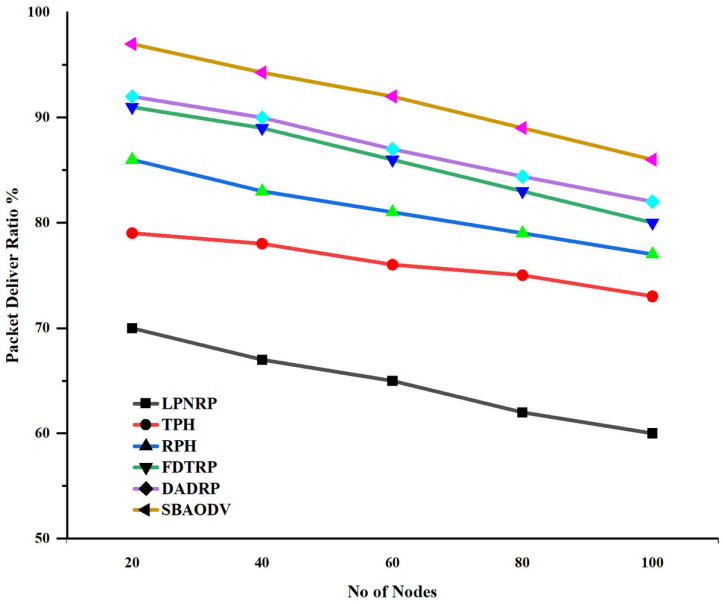


**Figure 6.** Packet delivery ratio % vs. no of nodes.

On the other hand, other protocols such as LPNRP, TPH, RPH, FDTRP, and DADRP show a decreasing trend in PDR% as the number of nodes increases. This may be because these protocols suffer due to the presence of black hole attackers, which destroys the paths and harms the devices as a result, the PDR% of other schemes decreases. In contrast, the proposed scheme adopted the Stackelberg game security model, efficiently detecting black hole attacks and maintaining the PDR% even at higher nodes.

Moreover, the proposed SBAODV protocol utilized the Stackelberg game model, which can detect black hole attacks and recover affected nodes in case of any attempt because of its best strategies. This feature enhances the network's security and ensures safe and reliable data transmission in IoMT networks. The results of this study can guide the selection of appropriate routing protocols for specific applications based on their performance characteristics and requirements. Further, the PDR% results justify the effectiveness of SBAODV routing protocol in IoMT-assisted UAV networks in ensuring the efficient and reliable transmission of data critical for improving the quality of healthcare services.

#### 4.3.2. Network Routing Load (%) vs. No of Nodes

Figure 7 shows the normalized data load for different routing protocols and network sizes in IoMT networks. A lower overhead value indicates a more efficient routing protocol. The results indicate that the SBAODV protocol has the lowest normalized load of data (overhead) across all network sizes tested. At 20 nodes, SBAODV has an overhead value of 2588, which is 20% to 30% lower than the other protocols, with DADRP being the closest with an overhead value of 2849. As the number of nodes increases, the overhead values for all protocols tend to increase. However, the SBAODV protocol maintains its superiority, with an overhead value of 5101 at 100 nodes, 7% to 23% lower than other existing routing protocols.

The low overhead value of SBAODV can be attributed to its ability to adapt to network topology changes and dynamically select the best path to the destination based on the available network resources. This enables the protocol to transmit data with the least amount of additional data, which can help reduce the UAVs' energy consumption and enhance the network's efficiency. In contrast, other protocols, such as LPNRP, TPH, RPH, FDTRP, and DADRP exhibit higher overhead values than SBAODV for all network sizes. These protocols are less efficient than SBAODV in transmitting data with the least amount of additional data. This is because of the Stackelberg game theory model SBAODV efficiently detect black hole devices and stops them from transmitting false packets across the network. While LPNRP, TPH, RPH, FDTRP, and DADRP cannot detect black hole attackers, these

devices transmit many false packets, increasing the network load across the network. From Figure 7, we can clearly observe that the proposed scheme offers the most negligible network load. These results highlight the importance of selecting an efficient routing protocol for IoMT networks assisted by UAVs. Efficient data transmission is critical for improving the quality of healthcare services provided. The low overhead value of SBAODV makes it a suitable choice for routing in these networks.

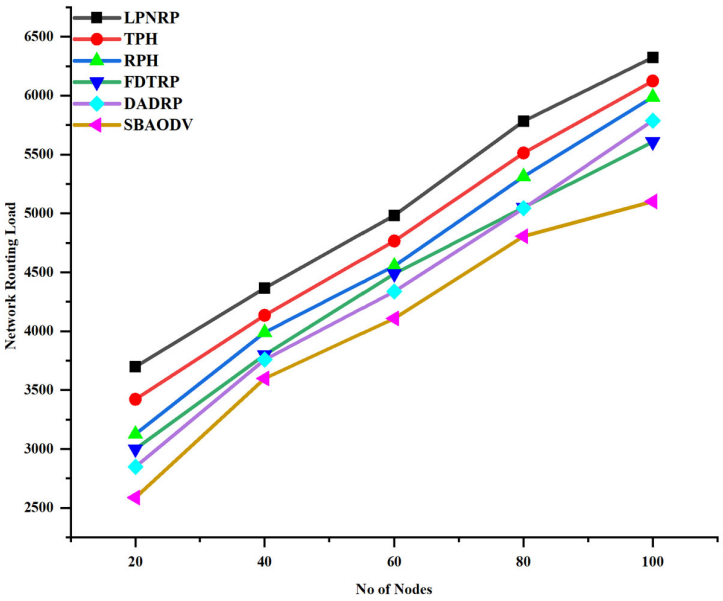


**Figure 7.** Network routing load vs. no of nodes.

#### 4.3.3. Throughput (kbps) vs. No of Nodes

Throughput is a crucial performance metric for IoMT networks, reflecting the network's capacity to transmit data efficiently. Figure 8, presented in the study, provides a detailed comparison of the throughput of different protocols and network sizes. The results indicate that the SBAODV protocol has the highest throughput values across all network sizes, ranging from 87.3 kbps for 20 to 77.7 kbps for 100 nodes. The high throughput values obtained by SBAODV can be attributed to its ability to adapt to network topology changes and dynamically select the best path to the destination based on the available network resources.

Comparing SBAODV with other protocols, it is evident that TPH, RPH, FDTRP, and DADRP exhibit lower throughput values than SBAODV for all network sizes. These protocols are not as efficient as SBAODV in capturing black hole devices and removing them from the network, which causes a reduction in their throughput values. On the other hand, LPNRP (routing protocol for low-power and lossy networks) demonstrates similar throughput values to SBAODV for all network sizes and maintains a throughput above 78%. However, other schemes suffer to maintain their throughput, with LPNRP offering the lowest values below 60% at 100 nodes. It is important to note that selecting a protocol for an IoMT network depends on various factors such as network topology, application requirements, and network reliability. At the same time, SBAODV has the highest throughput values compared to the other schemes because SBAODV utilizes a game theory algorithm, which makes it observe the behavior of end devices. If any device behavior is malicious, SBAODV utilizes the game model to block it as a result; other devices forward data efficiently through reliable routes, which increases the throughput of the proposed scheme. Further, the proposed scheme's result provides valuable insights into the performance of throughput as a result, the efficiency and quality of healthcare services in IoMT networks increase.

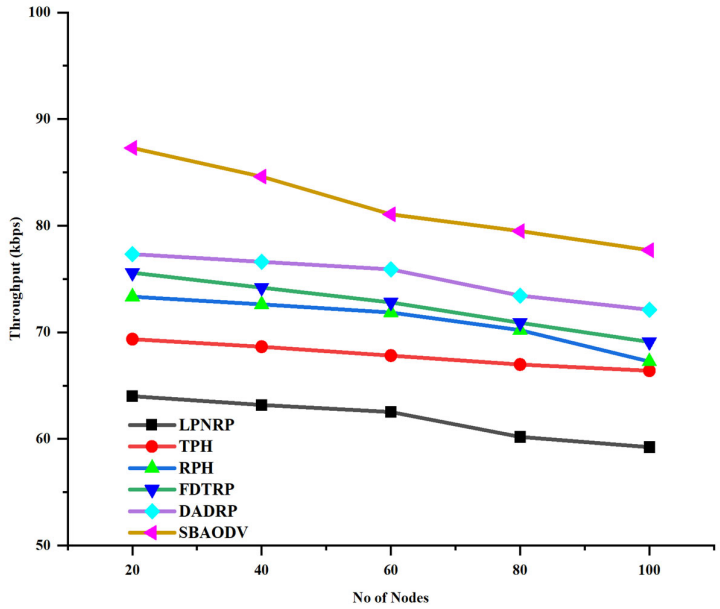


**Figure 8.** Throughput (kbps) vs. no of nodes.

#### 4.3.4. Detection Ratio % vs. No of Nodes

Figure 9 provides the results of the detection ratio % of the proposed SBAODV scheme compared to other routing protocols in IoMT networks. The detection ratio is an essential parameter that measures the capability of the routing protocol to detect malicious nodes present in the network. We can observe from Figure 9 that when the number of nodes in the network increases, the chances of malicious devices also increase. Therefore, it is crucial to detect them and ensure the safety of the network.

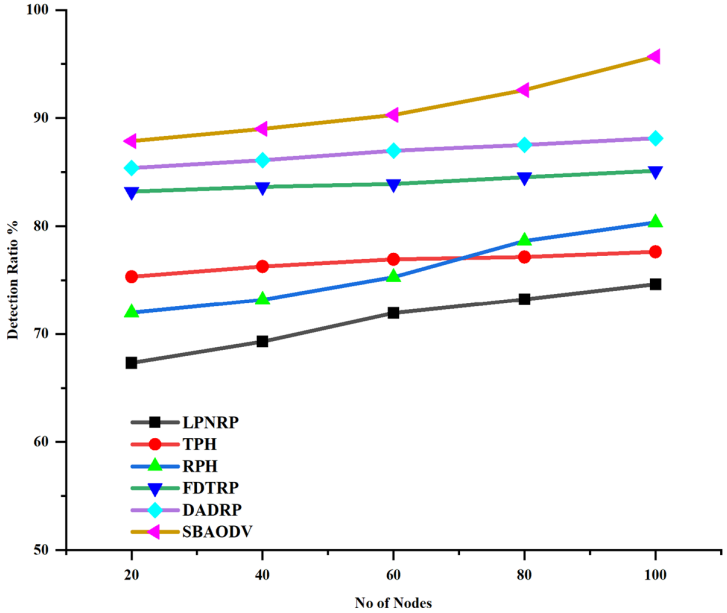


**Figure 9.** Detection ratio vs. no of nodes.

The Figure illustrates that as the number of nodes increases, the detection capability of SBAODV increases as well, reaching up to 95% at 100 nodes. The proposed SBAODV scheme outperforms other routing protocols with its excellent detection capability. This is due to the Stackelberg game theory algorithm, which observes the behavior of all devices and UAVs in case it recognizes any abnormal behavior. It utilizes the strong Stackelberg strategy to tackle the black hole attackers. Moreover, our proposed scheme can utilize pure and mixed strategies to

tackle the black hole attackers, providing a high detection ratio compared to all other schemes. On the other hand, DADRP provides the second-best results, with its detection ratio decreasing gradually as the number of nodes increases. The results of this study provide insight into the effectiveness of different routing protocols in detecting malicious nodes in IoMT networks, which can help improve the security of these networks.

#### 4.3.5. End-to-End Delay (ms)

End-to-end delay is one of the primary key metrics to measure the efficiency of routing protocol, which describes the time the packet takes to arrive at the destination node from the source. From Figure 10, we can observe that our proposed scheme offers an 18% delay at the initial point. While other schemes' delay at the initial point starts from higher values as the number of nodes increases, the delay also increases due to a high number of packets generated across the network, which causes the packet collision as well as packets lifetime expires before reaching the destination place. In IoMT networks due to the presence of black holes or rough devices, there is a chance these devices not only try to hack the data but also generate fake packets as a result, the collision occurs, which increases the delay across the network. Figure 10 shows that as the number of nodes increases, the delay for all routing schemes increases despite the increment in delay values. Our proposed SBAODV schemes maintain lower values up to 30% delay (ms), which we obtain at the highest number of nodes. On the other hand, benchmark schemes delay increases quickly as we can see from the results, the values increase in higher order. The proposed schemes take advantage of the Stackelberg game theory model to mitigate the rough devices efficiently; therefore, the information on reliable routes is available from the source to the destination node. Hence, the destination UAV finds the routes efficiently to decrease the delay while other schemes suffer, increasing their delay.

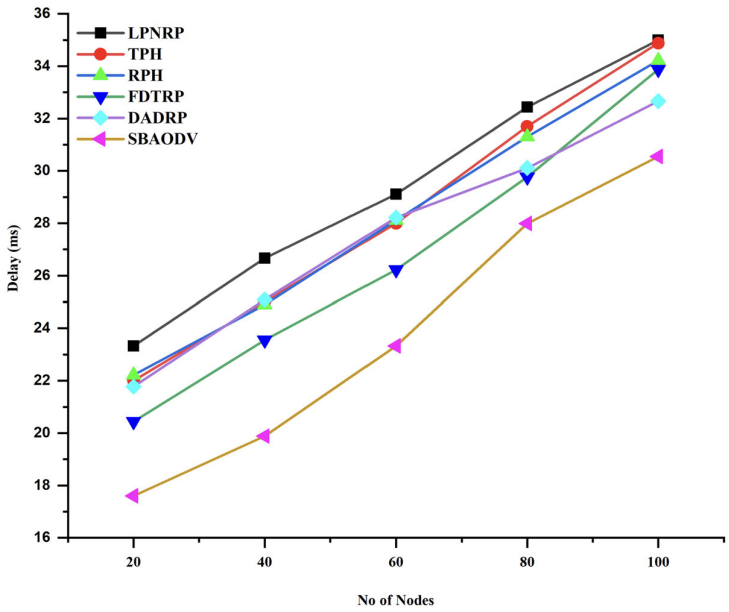


**Figure 10.** End-to-end delay (ms) vs. no of nodes.

### *4.4. Practical Discussions*

Using unmanned aerial vehicles (UAVs) and the Stackelberg game theory model can play a critical role in improving security and protecting privacy in disaster situations requiring rapid and accurate diagnosis and treatment of injured individuals. Whether it be a natural disaster such as a hurricane, tornado, or flood, or a human-made disaster such as a terrorist attack or mass casualty incident, the use of UAVs and the Stackelberg game theory model can be useful. Combining the Stackelberg game theory model with UAVs can help ensure efficient and secure communication between healthcare providers and emergency

responders. In the aftermath of a disaster, one of the main challenges facing healthcare providers and emergency responders is collecting and transmitting accurate medical data from the affected individuals. These data are critical for making informed decisions about how to treat patients and allocate resources. However, traditional communication networks may be unable to handle the volume of data transmission required in these situations and may also be vulnerable to cyberattacks and other security threats. This is where UAVs and the Stackelberg game theory model can make a significant difference. The UAVs can assist the patients and rescue centers with Internet of Medical Things (IoMT) devices, such as vital signs monitors, patient health records, and other medical sensors. These devices can collect and transmit data in real time to the UAVs, which can then relay the data to hospital centers and emergency response teams. This allows for more rapid and accurate diagnosis and treatment of injured individuals and can help to save lives in critical situations. The Stackelberg game theory model can also protect patient privacy and prevent unauthorized access to sensitive medical information. The model uses a lightweight encryption scheme that ensures secure data transmission between the UAVs and the IoMT devices, preventing third-party access to patient data.

Additionally, the hierarchical approach of the model allows UAVs to act as leaders in the game, making strategic decisions to optimize network performance and ensure secure data transmission. In contrast, IoMT devices act as followers, responding to the decisions made by the UAVs. Recently, an earthquake came to Turkey, which destroyed the main architecture of wireless networks it was critical to find the victims and offers first aid services and in this case, UAVs can play a crucial role in informing the rescue staff or hospitals about the patient's locations. Moreover, UAVs can also transport medical first aid staff to remote areas. In these scenarios, the patient's life is more important; therefore, it is necessary to have secure communication.

## 5. Conclusions

The IoMT-assisted UAV network is an emerging technology adopted in wireless networks to offer services in many practical scenarios. However, the fragile nature of UAVs makes it easy to attack the network. In this paper, we have investigated the black hole attacker scenario and proposed an SBAODV scheme to overcome this issue. The SBAODV routing scheme utilizes the Stackelberg game theory model for IoMT medical healthcare networks to protect patient data and reliable communication. We concluded that the security and safety of wireless networks can be significantly enhanced. Considering the competition between the attacker and the defender, the Stackelberg security game enables the defender to make informed decisions and effectively protect their resources. The proposed scheme consists of three main parts: the number of players, the set of strategies, and utility functions. The best response strategies for the defender and the attacker can be determined by analyzing the Nash equilibrium and strong Stackelberg equilibrium, leading to optimal outcomes for both parties. Using game theory models in healthcare networks can provide a robust and secure solution for protecting confidential medical data.

Future work can focus on further improving the proposed SBAODV scheme for securing IoMT-assisted UAV networks. This can include investigating its effectiveness under different attacks and network conditions, exploring its scalability and efficiency, and integrating machine learning and artificial intelligence techniques to enhance its performance. In addition, to ensure the highest level of security for IoMT systems and protect patient privacy and safety, researchers should consider multiple frameworks beyond the Stackelberg model, including risk assessment, vulnerability management, and regulatory compliance. The proposed SBAODV scheme can also be extended to other application domains beyond healthcare, such as industrial networks and smart cities, to provide a secure and reliable communication infrastructure.

**Author Contributions:** Conceptualization, J.A.S., C.W. and M.A.K.; methodology, M.A.K., S.U. and S.A.H.M.; software, S.A.C., M.S.A.M. and A.M.; validation, M.A.K. and S.A.H.M.; formal analysis, J.A.S. and M.A.K.; investigation, S.U. and S.A.C.; resources, M.A.K., M.S.A.M. and A.M.; data curation, C.W. and A.M.; writing—original draft preparation, J.A.S., C.W., M.A.K. and S.A.H.M.; writing—review and editing, J.A.S., C.W., M.A.K., S.A.H.M., M.S.A.M., S.A.C., S.U. and A.M.; visualization, S.U., S.A.C., M.S.A.M. and A.M.; supervision, C.W. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the Fundamental Research Funds for the Central Universities (No. 2022CDJYGRH-001) and the Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R239), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

**Data Availability Statement:** Not applicable.

**Acknowledgments:** The authors express This work is supported by the Chongqing Technology Innovation and Application Development Key Project (cstc2020jscx-dxwtBX0055; cstb2022tiad-kpx0148) and the authors express their gratitude to the Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R239), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

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

## References

1. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1646–1685. [CrossRef]
2. Rayan, R.A.; Zafar, I.; Tsagkaris, C. Iot technologies for smart healthcare. In *Advances in Data Science and Analytics: Concepts and Paradigms*; Wiley Online Library: Hoboken, NJ, USA, 2023; pp. 181–202.
3. Wagan, S.A.; Koo, J.; Siddiqui, I.F.; Qureshi, N.M.F.; Attique, M.; Shin, D.R. A fuzzy-based duo-secure multi-modal framework for IoMT anomaly detection. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 131–144. [CrossRef]
4. Wang, D.; Wu, M.; He, Y.; Pang, L.; Xu, Q.; Zhang, R. An HAP and UAVs Collaboration Framework for Uplink Secure Rate Maximization in NOMA-Enabled IoT Networks. *Remote Sens.* **2022**, *14*, 4501. [CrossRef]
5. Pasandideh, F.; da Costa, J.P.J.; Kunst, R.; Islam, N.; Hardjawana, W.; Pignaton de Freitas, E. A Review of Flying Ad Hoc Networks: Key Characteristics, Applications, and Wireless Technologies. *Remote Sens.* **2022**, *14*, 4459. [CrossRef]
6. Mohsan, S.A.H.; Othman, N.Q.H.; Li, Y.; Alsharif, M.H.; Khan, M.A. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intell. Serv. Robot.* **2023**, *16*, 109–137. [CrossRef] [PubMed]
7. Ullah, S.; Kim, K.-I.; Kim, K.H.; Imran, M.; Khan, P.; Tovar, E.; Ali, F. UAV-enabled healthcare architecture: Issues and challenges. *Future Gener. Comput. Syst.* **2019**, *97*, 425–432. [CrossRef]
8. Khan, M.A.; Kumar, N.; Mohsan, S.A.H.; Khan, W.U.; Nasralla, M.M.; Alsharif, M.H.; Żywiołek, J.; Ullah, I. Swarm of UAVs for Network Management in 6G: A Technical Review. *IEEE Trans. Netw. Serv. Manag.* **2022**, *20*, 741–761. [CrossRef]
9. Ali, M.; Qureshi, K.N.; Newe, T.; Aman, K.; Ibrahim, A.O.; Almujaly, M.; Nagmeldin, W. Decision-Based Routing for Unmanned Aerial Vehicles and Internet of Things Networks. *Appl. Sci.* **2023**, *13*, 2131. [CrossRef]
10. Rani, S.; Chauhan, M.; Kataria, A.; Khang, A. IoT equipped intelligent distributed framework for smart healthcare systems. *arXiv* **2021**, arXiv:2110.04997.
11. Khan, M.A.; Rehman, S.U.; Uddin, M.I.; Nisar, S.; Noor, F.; Alzahrani, A.; Ullah, I. An online-offline certificateless signature scheme for Internet of health things. *J. Healthc. Eng.* **2020**, *2020*, 6654063. [CrossRef]
12. Rouault, M.; Ejaz, W.; Naeem, M.; Masroor, R. The Role of UAV-Assisted IoT Networks in Managing the Impact of the Pandemic. *IEEE Commun. Stand. Mag.* **2021**, *5*, 10–16. [CrossRef]
13. Chamola, V.; Kotesh, P.; Agarwal, A.; Gupta, N.; Guizani, M. A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques. *Ad Hoc Netw.* **2021**, *111*, 102324. [CrossRef] [PubMed]
14. Tran, D.-H.; Nguyen, V.-D.; Chatzinotas, S.; Vu, T.X.; Ottersten, B. UAV relay-assisted emergency communications in IoT networks: Resource allocation and trajectory optimization. *IEEE Trans. Wirel. Commun.* **2021**, *21*, 1621–1637. [CrossRef]
15. Ullah, I.; Khan, M.A.; Khan, F.; Jan, M.A.; Srinivasan, R.; Mastorakis, S.; Hussain, S.; Khattak, H. An Efficient and Secure Multi-message and Multi-receiver Signcryption Scheme for Edge Enabled Internet of Vehicles. *IEEE Internet Things J.* **2021**, *9*, 2688–2697. [CrossRef]
16. Lv, Z.; Chen, D.; Feng, H.; Zhu, H.; Lv, H. Digital twins in unmanned aerial vehicles for rapid medical resource delivery in epidemics. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 25106–25114. [CrossRef] [PubMed]
17. Hossain, N.U.I.; Sakib, N.; Govindan, K. Assessing the performance of unmanned aerial vehicle for logistics and transportation leveraging the Bayesian network approach. *Expert Syst. Appl.* **2022**, *209*, 118301. [CrossRef]
18. Qassab, M.S.; Ali, Q.I. A UAV-based portable health clinic system for coronavirus hotspot areas. *Healthc. Technol. Lett.* **2022**, *9*, 77–90. [CrossRef]

19. Khan, M.A.; Shah, H.; Rehman, S.U.; Kumar, N.; Ghazali, R.; Shehzad, D.; Ullah, I. Securing internet of drones with identity-based proxy signcryption. *IEEE Access* **2021**, *9*, 89133–89142. [CrossRef]
20. Robinson, J.M.; Harrison, P.A.; Mavoa, S.; Breed, M.F. Existing and emerging uses of drones in restoration ecology. *Methods Ecol. Evol.* **2022**, *13*, 1899–1911. [CrossRef]
21. Tushar, W.; Yuen, C.; Saha, T.K.; Nizami, S.; Alam, M.R.; Smith, D.B.; Poor, H.V. A survey of cyber-physical systems from a game-theoretic perspective. *IEEE Access* **2023**, *11*, 9799–9834. [CrossRef]
22. Li, Y.; Wang, B.; Yang, Z.; Li, J.; Chen, C. Hierarchical stochastic scheduling of multi-community integrated energy systems in uncertain environments via Stackelberg game. *Appl. Energy* **2022**, *308*, 118392. [CrossRef]
23. Zhou, J.; Cao, Z.; Dong, X.; Vasilakos, T. GTSIM-POP: Game theory based secure incentive mechanism and patient-optimized privacy-preserving packet forwarding scheme in m-healthcare social networks. *Future Gener. Comput. Syst.* **2019**, *101*, 70–82. [CrossRef]
24. Messous, M.-A.; Senouci, S.-M.; Sedjelmaci, H.; Cherkaoui, S. A game theory based efficient computation offloading in an UAV network. *IEEE Trans. Veh. Technol.* **2019**, *68*, 4964–4974. [CrossRef]
25. Khan, M.A.; Menouar, H.; Eldeeb, A.; Abu-Dayya, A.; Salim, F.D. On the detection of unauthorized drones-techniques and future perspectives: A review. *IEEE Sens. J.* **2022**, *22*, 11439–11455. [CrossRef]
26. Taleb, T.; Sehad, N.; Nadir, Z.; Song, J. VR-based Immersive Service Management in B5G Mobile Systems: A UAV Command and Control Use Case. *IEEE Internet Things J.* **2022**, *10*, 5349–5363. [CrossRef]
27. Bae, J.; Sohn, K.Y.; Lee, H.; Lee, H.; Lee, H. Structure of UAV-based Emergency Mobile Communication Infrastructure. In Proceedings of the 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 20–22 October 2021; pp. 634–636.
28. Ejaz, W.; Ahmed, A.; Mushtaq, A.; Ibnkahla, M. Energy-efficient task scheduling and physiological assessment in disaster management using UAV-assisted networks. *Comput. Commun.* **2020**, *155*, 150–157. [CrossRef]
29. Rottondi, C.; Malandrino, F.; Bianco, A.; Chiasserini, C.F.; Stavrakakis, I. Scheduling of emergency tasks for multiservice UAVs in post-disaster scenarios. *Comput. Netw.* **2021**, *184*, 107644. [CrossRef]
30. Ullah, S.; Mohammadani, K.H.; Khan, M.A.; Ren, Z.; Alkanhel, R.; Muthanna, A.; Tariq, U. Position-Monitoring-Based Hybrid Routing Protocol for 3D UAV-Based Networks. *Drones* **2022**, *6*, 327. [CrossRef]
31. Lu, X. Implementation of art therapy assisted by the internet of medical things based on blockchain and fuzzy set theory. *Inf. Sci.* **2023**, *632*, 776–790. [CrossRef]
32. Zhao, N.; Lu, W.; Sheng, M.; Chen, Y.; Tang, J.; Yu, F.R.; Wong, K.-K. UAV-assisted emergency networks in disasters. *IEEE Wirel. Commun.* **2019**, *26*, 45–51. [CrossRef]
33. Ma, B.; Wu, J.; Liu, W.; Chiaraviglio, L.; Ming, X. Combating hard or soft disasters with privacy-preserving federated mobile buses-and-drones based networks. In Proceedings of the 2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI), Las Vegas, NV, USA, 11–13 August 2020; pp. 31–36.
34. Gupta, L.; Jain, R.; Vaszkun, G. Survey of important issues in UAV communication networks. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1123–1152. [CrossRef]
35. Islam, A.; Shin, S.Y. BUAV: A blockchain based secure UAV-assisted data acquisition scheme in Internet of Things. *J. Commun. Netw.* **2019**, *21*, 491–502. [CrossRef]
36. Cheng, N.; Wu, S.; Wang, X.; Yin, Z.; Li, C.; Chen, W.; Chen, F. AI for UAV-Assisted IoT Applications: A Comprehensive Review. *IEEE Internet Things J.* **2023**, 1. [CrossRef]
37. NS2. The Network Simulator—Ns-2. Available online: https://www.isi.edu/nsnam/ns (accessed on 1 April 2023).
38. Mohammadani, K.H.; Memon, K.A.; Memon, I.; Hussaini, N.N.; Fazal, H. Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks. *Int. J. Distrib. Sens. Netw.* **2017**, *16*, 15501477209. [CrossRef]
39. Khalifeh, A.F.; AlQudah, M.; Darabkh, K.A. Optimizing the Beacon and SuperFrame orders in IEEE 802.15.4 for real-time notification in wireless sensor networks. In Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 22–24 March 2017; pp. 595–598.
40. Bouzebiba, H.; Lehsaini, M. FreeBW-RPL: A New RPL Protocol Objective Function for Internet of Multimedia Things. *Wirel. Pers. Commun.* **2020**, *112*, 1003–1023. [CrossRef]
41. Lenin, A.H.; Vasanthi, S.M.; Jayasree, T. Automated Recognition of Hand Grasps Using Electromyography Signal Based on LWT and DTCWT of Wavelet Energy. *Int. J. Comput. Intell. Syst.* **2020**, *13*, 1027–1035. [CrossRef]
42. Saba, T.; Haseeb, K.; Ahmed, I.; Rehman, A. Secure and energy-efficient framework using Internet of Medical Things for e-healthcare. *J. Infect. Public Health* **2020**, *13*, 1567–1575. [CrossRef] [PubMed]

43. Refaee, E.; Parveen, S.; Begum, K.M.J.; Parveen, F.; Raja, M.C.; Gupta, S.K.; Krishnan, S. Secure and Scalable Healthcare Data Transmission in IoT Based on Optimized Routing Protocols for Mobile Computing Applications. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 5665408. [CrossRef]
44. Ali Zardari, Z.; He, J.; Zhu, N.; Mohammadani, K.H.; Pathan, M.S.; Hussain, M.I.; Memon, M.Q. A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs. *Future Internet* **2019**, *11*, 61. [CrossRef]