The limitations in the state-of-the-art counter-measures against the security threats in H-IoT

Yazdan Ahmad Qadri, Rashid Ali, Arslan Musaddiq, Fadi Al-Turjman, Dae Wan Kim & Sung Won Kim

Cluster Computing
The Journal of Networks, Software Tools and Applications

ISSN 1386-7857
Volume 23
Number 3

Cluster Comput (2020) 23:2047-2065
DOI 10.1007/s10586-019-03036-7

Springer

Cluster Computing (2020) 23:2047–2065
https://doi.org/10.1007/s10586-019-03036-7

The limitations in the state-of-the-art counter-measures against the security threats in H-IoT

Yazdan Ahmad Qadri[1] · Rashid Ali[2] · Arslan Musaddiq[1] · Fadi Al-Turjman[3] · Dae Wan Kim[4] · Sung Won Kim[1]

Received: 8 June 2019 / Revised: 10 October 2019 / Accepted: 19 December 2019 / Published online: 1 January 2020

Abstract
Internet of Things (IoT) technology is anticipated to pave the way for groundbreaking applications in a number of areas of current healthcare systems. Given the significant number of connected medical devices, the vital data generated by the patient is under several security threats. Selective Forwarding (SF) and Wormhole (WH) attacks are two critical threats that cause information deficit in the network. The SF attack drops critical data packets at compromised nodes while the WH attack creates fallacious routing tables due to the introduction of malicious routes in the network. In this paper, we focus on the security aspects of Healthcare-IoT and review the proposed counter-measures against the SF and WH attacks. We weigh the recently postulated counter-measures based on their significance and identify their limitations. Additionally, we propose a blockchain-based cryptographic framework for mitigating SF and WH attacks in H-IoT. We explore future research directions in mitigating these threats.

Keywords Healthcare IoT · Selective forwarding attack · WBANs · Wormhole attack · Blockchain technology

1 Introduction

Internet of Things (IoT) encompasses both the physical things and digital information combined over a communication network. When wearable sensors and medical actuators send sensed data over the IoT for healthcare purposes, it constitutes a Healthcare Internet of Things (H-IoT) [1]. The sensors perform the ubiquitous monitoring of vital human body functions. The vital parameters, like blood glucose level, blood oxygen level, blood pressure, body temperature, and electrocardiogram, are monitored. Such systems are becoming increasingly popular in relieving the pressure on the hospitals, where a majority of patients are under observation. H-IoT covers areas such as Ubiquitous Health Monitoring (UHM), Computer-Assisted Rehabilitation (CAR), Emergency Medical Response System (EMRS) and lifestyle tracking [2]. It has been estimated that over 50 billion devices would be connected to the internet by 2020 [3] through IoT technology. The exponential proliferation of connected healthcare devices in H-IoT also invites multiple security risks. Therefore, steps are taken to mitigate these risks without affecting the Quality of Service (QoS) [4].

✉ Sung Won Kim
swon@yu.ac.kr

Yazdan Ahmad Qadri
yazdan@ynu.ac.kr

Rashid Ali
rashidali@sejong.ac.kr

Arslan Musaddiq
arslan@ynu.ac.kr

Fadi Al-Turjman
fadi.alturjman@antalya.edu.tr

Dae Wan Kim
c.kim@ynu.ac.kr

[1] Department of Information and Communication Engineering, Yeungnam University, Gyeongsan 38541, Republic of Korea

[2] School of Intelligent Mechatronics Engineering, Sejong University, Seoul, Republic of Korea

[3] Artificial Intelligence Department, Near East University, 99138 Nicosia, Mersin, Turkey

[4] Department of Business Administration, Yeungnam University, Gyeongsan 38541, Republic of Korea

A network of sensors and actuators associated with human bodies, connected over a radio network, is known as a Wireless Body Area Network (WBAN). A WBAN collects the physio-chemical data of the human body with the help of the attached sensors to provide artificial stimuli [2]. A typical WBAN architecture follows a three-tier architecture [5] as depicted in Fig. 1. As shown in the figure, the first layer includes sensors and actuators to collect information from the environment (human body or surrounding) and is known as the sensor/device layer. It consists of wearables or implants that can measure physiological data called Patient-Generated Data (PGD). Several advanced wearables measure parameters such as body temperature, blood pressure, blood glucose level, hormonal levels, and electrocardiogram. These sensors send the data via a gateway or a base station (BS) such as a smartphone or a personal digital assistant (PDA) [6]. At the device layer, Bluetooth Low Energy (BLE) [7], ZigBee [8] and Wi-Fi [9] are the most popular communication technologies that are used to transmit data from the end devices to the gateway/BS. The PGD received at the gateway/BS can be pre-processed at the Edge node/Fog node before being sent to the cloud or server. Edge computing, extends the intelligence of the cloud to the edge of the network, by utilizing the end-user device or edge device for storage, communication, and processing [10]. The edge node may also be an intelligent network device such as a switch, which can perform computing operations in real-time and provide support for the low latency applications. An efficient interaction among the fog nodes ensures a reliable data delivery and service [11]. The transmission layer of a WBAN architecture constitutes long-range links that connect the network gateway to the cloud or the servers, as shown in Fig. 1. Long-range and low power communication technologies such as Low Power Wide Area Network (LoRaWAN) [12], Sigfox [13] and Narrowband (NB-IoT) [14] have been successfully deployed in this layer [15, 16]. These communication technologies are used to bring pre-processed data to the third layer, the cloud servers for storage and analytics. The analytics help in the modeling of physiological processes in the human body and diagnosis [17]. The transmission is guided by the use of low power consuming routing protocols at the network layer in the WBANs which allows higher energy efficiency and low latency [18, 19]. The distributed nature of the WBANs allows the compliance with the QoS for the H-IoT systems [20, 21]. The introduction of the Internet of Nano-Things (IoNT) is accelerating the proliferation of the massive IoT deployment especially as WBANs, therefore, amplifying the security challenges [22, 23]. Additionally, Network Function Virtualization (NFV), is transforming the network management by powering a paradigm shift in the resource allocation, network security and network flexibility [24].

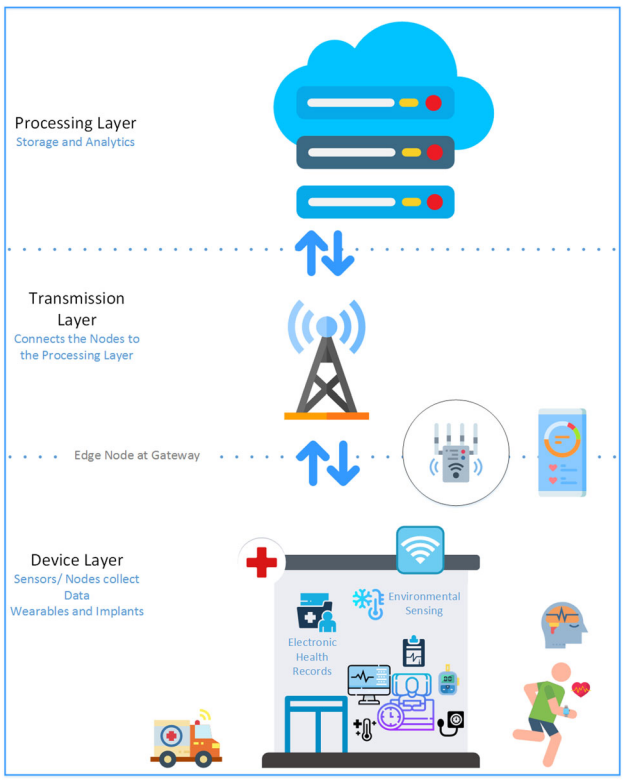

Fig. 1 A typical 3-tier architecture of H-IoT

A range of security mechanisms secures the transmission of data between the three layers. However, some loopholes and vulnerabilities can be exploited to listen to PGD without authorization. These weaknesses can also be used to interrupt the data stream, introduce malicious data, or even bring the entire system down. Selective forwarding (SF) attack [4] is one of the threats, which is responsible for creating an information deficit in the network by dropping selective data packets during transmission. Similarly, another security threat, known as Wormhole (WH) attack [4] tries to disrupt the transmission routes by creating unauthorized links within a network. Therefore, it becomes essential for the academic as well as an industrial research community to identify such loopholes and provide appropriate countermeasures against such attacks.

In this paper, we comprehensively study the current research work related to the security issues in H-IoT (with a broader view of IoT). Based on the related research works, we briefly describe some of the security challenges, mainly due to SF and WH attacks. To mitigate these security issues, we propose to use the blockchain [26] technology-based framework. Blockchain is an emerging technology that has attracted the interests of academic as well as industrial researchers across a wide span of applications, such as healthcare [27]. The reason for a peak in interest in blockchain is because, with blockchain

technology, applications that previously required trusted central nodes, can now operate in a fully decentralized and trustful manner, without the need for a central node, and achieves the same functionality with similar performance [28]. Therefore, we propose a blockchain-based framework for mitigating SF and WH attacks in H-IoT. The highlights of the contributions of this paper are as follows,

- A brief discussion of security challenges to the H-IoT with a focus on SF and WH attacks.
- A comprehensive literature review related to the SF and WH security issues in IoT.
- Analysis of the current counter-measures against the SF and WH attacks that highlights their limitations.
- The possible directions for future research in H-IoT network security.
- Finally, we propose a blockchain-based cryptographic framework for mitigating SF and WH attacks in HIoT.

The organization of the remaining paper is as follows. Section 2 discusses the different threats faced during the transmission of data. Section 3 explores the related research work done for the appropriate counter-measures. Based on the limitations of current counter-measures, the future research directions are sketched out in Sect. 4. A proposal for a blockchain-based framework for mitigating the SF and WH attacks in H-IoT is included in Sect. 5. Section 6 concludes the discussion. Table 1 shows a list of abbreviations used in this paper.

Table 1 List of abbreviations acronyms used in this paper

Acronyms	Full description
AODV	Adhoc on-demand distance vector
BS	Base station
CAR	Computer assisted rehabilitation
DOS	Denial of service
EMRS	Emergency medical response system
ETX	Emergency medical response system
H-IoT	Healthcare Internet of Things
IDS	Intrusion Detection System
IoT	Internet of Things
MANET	Mobile adhoc network
PGD	Patient generated data
QoS	Quality of service
RDC	Radio duty cycle
RPL	Routing protocol for low power & lossy networks
RTT	Round trip time
SF	Selective forwarding attack
TCP	Transmission control protocol
UHM	Ubiquitous health monitoring
WBAN	Wireless body area networks
WH	Wormhole attack

2 Security challenges

The security level of a network can be traditionally judged based upon three key factors: (1) confidentiality, which is maintaining the secrecy of the data, (2) integrity, which stands for maintaining the original form of the data and (3) availability, which determines the access to the data at any instant for authorized users. The transmission layer of the H-IoT architecture is responsible for the transmission of data from sensors to the cloud or servers. At this layer, numerous threats can undermine the authenticity and integrity of the data. As shown in Fig. 2, the threats at the network layer of WBAN technologies are classified as either, (1) internal attacks or (2) external attacks [5]. The internal attacks affect the nodes from within the network, that is, either a legitimate node is compromised, or a malicious node is introduced. These nodes may also have cryptographic information about the network and are, therefore, able to obtain private data. Since the malicious node has the trust of the network, it is a very challenging task to identify the internal attacks. While on the other hand, external attacks can be launched from outside the network. In an external attack, no internal information about the network such as cryptographic keys or node identity is available to the attacker [29].

Tomić et al. [25] identified various threats and their mode of operation at the network layer of the WBAN in an IoT network. Figure 2 provides an insight into the classification of various attacks according to their categories at the WBAN network layer. Numerous efforts have been made to propose counter-measures to tackle these security threats. In this paper, we focus on SF and WH attacks, which fall under internal threats at the WBAN network layer. These attacks are difficult to detect, as their effects can be similar to the network disruptions caused by factors like weak channel, poor link quality, and node failure or even energy constraints. There is an increased threat of compromising the highly sensitive patient-generated data during these two attacks. Additionally, it has been observed that the WH attack is accompanied by attacks [30]. Thus, its detection could help in securing the network from a range of network layer attacks too. Therefore, owing to the severity of these threats, we discuss the nature of these attacks, their significance, and their counter-measures in detail.

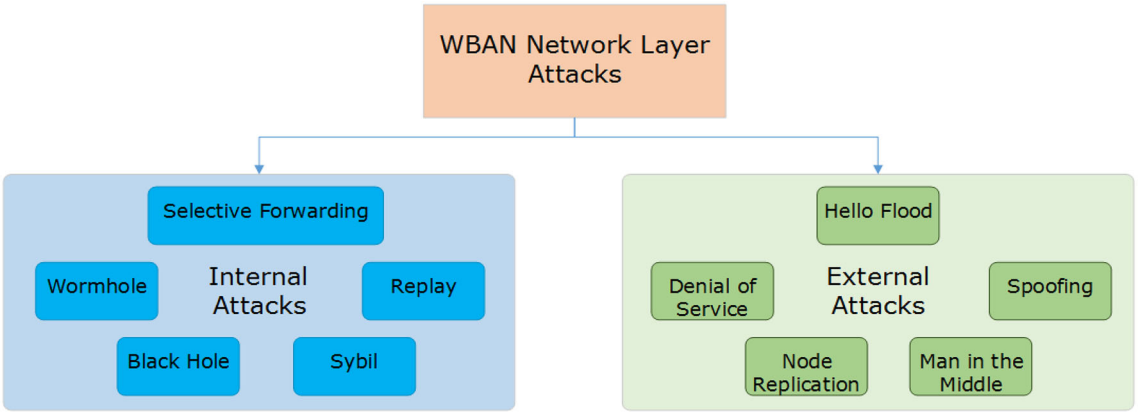

Fig. 2 Classification of WBAN network layer attacks [25]

2.1 Selective forwarding attack

In an SF attack, a malicious node drops selective packets from specific internal nodes. Whereas, if the malicious node blindly drops all the packets, it is called a Black Hole attack [31]. Figure 3 depicts the operation of an SF attack in WBAN. SF attack is difficult to detect as there can be several reasons for the packet dropping, such as an unreliable channel or medium access collisions; hence, careful analysis is required for the detection of SF attack. The malicious node can selectively forward packets with reliability, therefore suppressing the suspicion about the errors in routing protocols. Several measures have been presented for the detection and mitigation of SF attack by using different features of an IoT network. In the next section, we cover a comprehensive review of the counter-measures against SF attacks.

2.2 Wormhole attack

The nature of WH attack is passive, which creates a malafide link between two points (nodes), usually itself to the malicious node, within the network. Wormhole attack creates a high-quality wireless link between the target nodes for the construction of a WH tunnel as shown in Fig. 4. In WH, an attacker creates tunnel either by using encapsulation, creation of out-of-band channels, or by high power transmission. If an attacker is able to execute a WH attack, there is a high probability that malicious nodes can use it for traffic analysis. The attacker can also cause a Denial-of-Service (DoS) attack by dropping certain data or control packets [32].

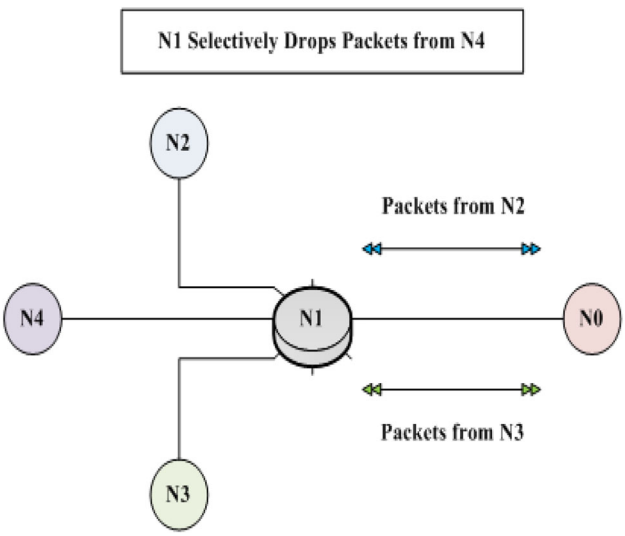

Fig. 3 Operation of selective forwarding attack

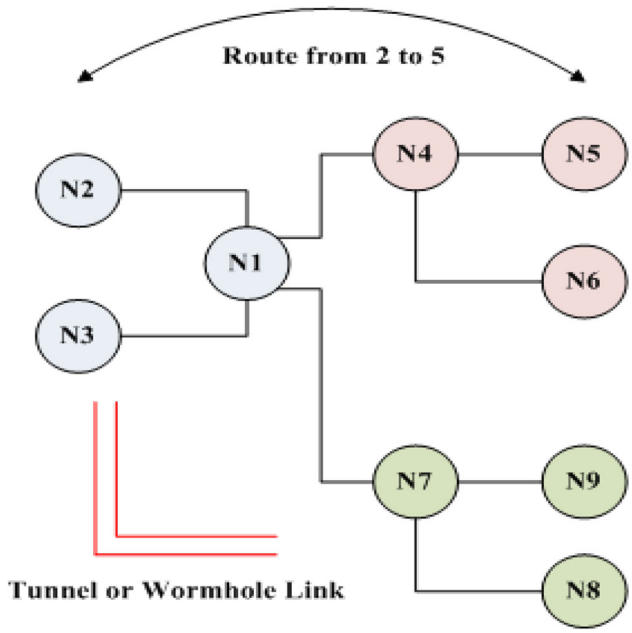

Fig. 4 Wormhole attack in a network

3 The counter measures against the selective forwarding and wormhole attacks

In this section, a comprehensive review of the counter-measures against SF and WH attacks in WBAN is present. The pros and cons of the different methodologies are weighed upon, and the limitations of these counter-measures are identified. The various authors have proposed multiple approaches, that include manipulating the existing standards and protocols. Additionally, modern techniques like machine learning (ML)are also exploited.

Bo et al. [33] present a scheme for the detection of the SF attack using a mechanism with three types of packets; report packet, acknowledgment packet, and alarm packet. The detection of an attack includes upstream and downstream detection tasks that are implemented by the uncompromised nodes according to their respective positions. All the nodes in the routing path are responsible for attack detection. In an upstream process, a report packet is generated when an unusual event takes place in the network. The report packet sets a counter to a pre-defined metric which decrements at each hop during the report packet's journey to the destination node. Each node decrements a tracking counter after forwarding the report packet to the next hope. If the counter reaches zero at any node, an acknowledgment packet is sent by the node to the actual sender of the report packet via the same path. Once the report packet and the previous acknowledgment packet from the nodes along the path are received before the stipulated time, an acknowledgment packet is sent; otherwise, an alarm packet is sent to the source node, which retransmits the data. The failure to receive the acknowledgment packets helps in creating the suspicious node list. On the other hand, the downstream process generates alarm packets to inform the sender if there is any suspicious node in the network. In this counter-measure, the message overhead associated with the data is a major drawback, and it increases smoothly with an increased number of connected nodes.

Liu et al. [34] propose an SF attack detection scheme that utilizes a per-hop acknowledgment (PHACK) mechanism to detect the malicious node. Their proposed methodology detects the SF attack effectively and enables the network to recover from the attack. In this approach, all the intermediate nodes along the route are required to send an acknowledgment of the received packet. In this mechanism, single path failure is averted by utilizing multiple paths to send the confirmation information to the sink node. The PHACK based approach is also able to identify the suspicious nodes and removes the suspicious nodes from the forwarding path. The data packets are rerouted and resent in an attempt to recover the lost data. The detection accuracy of this method is high, but the energy consumption at the network hotspots remains unimproved as compared to the previous techniques. The performance evaluation results show an increase in energy usage at the periphery of the network. Furthermore, this scheme is not apposite for mobile WSN's. Therefore, it is not suitable for H-IoT applications where the subjects are mobile.

Mathur et al. [35] postulated a detection and defense mechanism against the SF attack. They proposed a modified Ad-hoc On-Demand Distance Vector (MAODV) routing protocol to shift the control from the source node to the BS, enhancing trust and energy efficiency. The Radio Duty Cycle (RDC) layer is also modified to aid the detection capabilities of this mechanism. All upstream and downstream data packets traveling through these nodes can be monitored for SF attack. The mitigation process is aided using a control packet (CP), a timer, and a threshold. The timer is set after an aggregated CP is forwarded to the next node. If the CP fails to reach the subsequent node during the threshold period, the CP is broadcasted in the network until it reaches the intended destination node via a redundant route. However, the nodes, which reside far from the BS, are prone to high latency that can prove detrimental to the healthcare applications.

Ren et al. [36] presented a Channel Aware Reputation with Adaptive Threshold (CSR-A) method for the detection and localization of the SF attack. It detects the attack by comparing the estimated packet loss with the actual packet loss in the network between the nodes. Each node in the network maintains a reputation table, which determines the reliability of a node in the network. The average lifetime of a network is divided into time slots called the evaluation periods. Each evaluation period starts with the channel estimation step, during which the packet loss rate is evaluated. The evaluation period ends with the reputation update in which the reputation table is updated with the reputation metrics of the node. Since the link quality of the node at different areas is varied, an adaptable threshold value is calculated. If the node reputation falls above this threshold, the node is included in the routing path else it is left out. This methodology can be applied to any routing protocol. It has a significant detection accuracy and improves the data delivery ratio by 10%. However, there is a considerable calculation overhead associated with the technique and requires computational power and storage capabilities for reputation tables.

An Intrusion Detection System (IDS) has been proposed by Gara et al. [37]. It is focused on intrusion detection in mobile WSN's based on IPv6 Routing Protocol for Low Power & Lossy Networks (RPL). This technique combines the use of the Sequential Probability Ratio Test (SPRT) and the adaptive threshold of acceptable probability of dropped

packets based on Expected Transmission Count (ETX). The process consists of four steps. The first step includes the collection of neighborhood information by sending and receiving "hello" packets. The second step, called the data analysis step involves computing the number and probability of packet drops. A node is quarantined if the probability exceeds the threshold value, which is calculated by using ETX. The decision step aims to detect malicious nodes and minimize the number of legitimate nodes detected as malicious, and the number of malicious nodes detected as legitimate nodes. SPRT is used to find compromised and legitimate nodes. The final step is the elimination step that entails the removal of malicious nodes from the routing path. The simulations have shown promising results with a 100% detection rate but at the expense of a large overhead.

In certain SF attacks, a malicious node may only try to disrupt a particular data flow instead of all the flows through that node. This type of attack is termed as the Selective Gray Hole attack (SGHA). The proposed method by Prabhakar et al. [31] is aimed at detecting the SGHA and improving the data delivery ratio for wireless multi-hop networks in IoT systems. Each node monitors the downstream traffic in an attempt to detect the SGHA. All the nodes maintain two reputation tables to evaluate the flow of the downstream nodes neighboring it. The tables contain short-term and long-term reputation scores of the neighboring nodes, which are updated continuously based on the network dynamics. The network is evaluated throughout its lifetime. The lifetime is divided into evaluation slots during which the conditions of the channel remain constant. During each slot, the reputation is updated using the following steps.

1. *The reputation evaluation* It is also known as the First-Hand Reputation. The upstream nodes evaluate the reputation score by calculating the packet loss. A counter is used to monitor the number of packets sent by the upstream node to the downstream node and also the number of packets that the downstream node forwards further. The packet loss helps in calculating the short-term reputation score.
2. *The reputation propagation* This score is also called Second-Hand Reputation. It contributes to the calculation of short-term reputation score. The nodes are assigned priorities and weights based on their reputation scores calculated earlier and their vicinity to the gateway or cluster head.
3. *Reputation integration* The short-term score evaluated during the above two steps is used to formulate the long-term score, which takes into account the previous behavior of the node. Thus, if the compromised node implements a strategy to intermittently drop a flow in order to suppress the suspicion of its malicious intents, the proposed IDS would still be able to detect the attack.
4. *Identification of the malicious node* The reputation tables are sent to the gateway periodically based on the algorithm. The reputation scores are compared with the threshold limits. If the deviation is within the permissible limits, the nodes remain in the flow; otherwise, the neighboring nodes are informed about the identity of the malicious node and removed from the flow.

This approach successfully identifies the SGHA, which is usually hard to detect for the traditional approaches. The overhead and the computing limitations imposed by the design of the H-IoT challenge the suitability of this mechanism for such applications. The maintenance of reputation tables is energy-intensive process and requires additional storage capabilities.

Ioannou et al. [38] postulate an anomaly-based intrusion detection system called mIDS. The mIDS system supports multi-layer monitoring of the sensors and takes into consideration the locally generated data of the sensors. A statistical modeling tool known as Binary Logistic Regression (BLR) is used for sensor parameter classification. The proposed method collects network parameters like data packets received, data packets sent, packets forwarded, packets dropped, and announcements received. These values constitute a vector, and a vector is created for each run. The anomaly detection system involves the creation of a network profile based on the above-stated network parameters at the time of network deployment. A profile for a normal or benign scenario as well as the viral or malignant scenario is prepared. A Runtime Management Tool (RMT) collects the vectors at periodic intervals. The vectors are compared with the standard profiles. If the vector trespasses the thresholds, the network is classified as malignant. The BLR is used to classify the network activity based upon independent variables, which constitute the network parameter vector. The BLR goes through a training phase, and then evaluation is carried out after intervals. The accuracy of this approach lies in the range of 88–100%, based on various test runs in different scenarios. One of the advantages of this system is that it does not require the sensors to be online for the detection of intrusion. The locally generated parameters are evaluated for the detection of intrusion. This reduces network traffic and overhead. However, the computing capabilities of sensors are minimal, and thus, it is not feasible to implement this system at the client level. The clustering approach can be taken up for such applications. Additionally, a significant number of false alarms were reported during the evaluation. For a large-scale deployment of a critical IoT system, false alarms can cause performance degradation. The

flawed models at deployment can affect the detection accuracy.

Dorri [39] propose a mechanism for detecting and mitigating Blackhole (BH) attacks in MANETs. BH attacks are a subset of SF attacks in which all the data packets are blindly dropped by the malicious nodes. The proposed scheme aims at eliminating the attack caused by co-operating malicious nodes, which help in each other to evade the commonly used counter-measures. The proposed method is based on the use of an additional data-packet type control packet and an Extended Data Routing Information (EDRI) table. The approach is designed over the AODV protocol in MANETs. The transmission control protocol (TCP) is used for the transmission of the proposed control packet. The EDRI table contains information of the neighboring nodes, previously neighboring nodes and the nodes classified as malicious. Each node maintains this table and advertises it to the neighbors. The Proposed Control Packet (PCP) appears like a data packet, which is usually dropped by the malicious node but may forward this packet to the co-operating malicious nodes. The malicious nodes, usually to avoid suspicion, transmit the ordinal Control Packet (CP). Therefore, by knowing which nodes forward both types of packets, it could be determined if the forwarding node is secure or a malicious node. Each node updates the other nodes about its next-hop neighbors (NHN) and sends the EDRI tables of their NHNs along with the control packets. The PCP also contains a random number that remains constant for all nodes. The nodes which do not forward the PCP are contacted with an ordinal CP. The proposed security mechanism has the following three steps; (1) determining a freshest path, which introduces the NHNs of each node (2) checking the freshest path, which involves validating the metrics in the PCP and CP and (3) eliminating malicious nodes from the forwarding path, which is essentially removing the malicious nodes from the network and adding their ID to the BH nodes list. This approach can detect collaborative BH attacks reliably. However, the delay and overhead can be improved for a critical IoT system.

Pu et al. [40] propose a three-tier solution. Firstly, a single checkpoint counter-measure called SCAD is used. Secondly, it includes the utilization of timeout and hop-by-hop retransmission technique for the recovery of unexpectedly lost packets caused by the forwarding misbehavior or poor channel. Thirdly, their method is aided using the alarm packet. The packet forwarding nodes on the routing path receives the acknowledgment packets. These nodes verify the authenticity of the acknowledgment packets from the source information. To aid in its accuracy a timer is set, during which the acknowledgment packet should be received otherwise an alarm packet is sent. This entire method attracts an increasing computational overhead, and it is not highly effective in active detection as multiple colluding malicious nodes can bypass this system.

Mehetre et al. [41] propose a secure and trusted routing scheme with an aim to identify and avoid malicious nodes based on active trust for cluster WSN. This protocol computes a secure and trusted route from source to destination for the WSNs. It is founded on three principal steps viz. detection of malicious nodes, securing the packets, and finding a secure route. The use of Detection Packet (DP) for node detection is coupled with a trust mechanism. Then, a dual assurance scheme is employed which includes a Selective Forwarding-based packet validation, and the data from the source node is encrypted using the elliptic curve cryptography (ECC) to make the forwarded data packet secure. A secure routing path is identified in the entire path transmission using the trust path selection, and Cuckoo Search (CS) algorithm. This algorithm provides an energy-efficient and reliable counter-measure against SF attack. The comparative analysis showed a satisfactory performance, but the latency incurred was not suitable for healthcare applications that essentially should be minimal.

Khabbazian [32] propose a timing-based measurement approach for the WH attack detection algorithm. Each node validates its neighbors in two round communication-process. The first round comprises of every node sending a signed "Hello" message and recording the time information. This message contains the sender ID and a nonce. After sending the "Hello" message, each node obtains the list of its neighbors. In the second communication round, the response messages are exchanged which include the following information; (1) Time at which the node's "Hello" message was sent, (2) The list of all the ID's in the received Hello messages along with their corresponding nonce and (3) The times at which they were received. These messages are termed as "follow-up packets." This collected time information is used to estimate the distance between the nodes. When a node receives the "follow-up" packet, it first checks its corresponding nonce in the packet and verifies the sender's signature. It then calculates the time for the two-round transmissions using 1.

$$\frac{(t_{y,x} - t_y) - (t_x - t_{x,y})}{2} \times c \leq T_{max}, \tag{1}$$

where t_x is the sending time of node x's "Hello" message recorded by node x, $t_{x,y}$ is the receiving time of node y's "Hello" message recorded by node x and T_{max} is the maximum transmission range. Similarly, $t_x - t_{x,y}$ is the delay between the time when node y's "Hello" packet is received at node x. If the response packet is received within the T_{max}, a neighborhood relationship is established. This method does not require synchronized clocks, and there is no requirement for one-to-one communication with the neighbors, which increases the computational load.

However, this method depends on the assumption that the time at which the packets are sent and received is known and the communication takes place at the speed of light.

Modirkhazeni et al. [42] propose that a pre-shared key be distributed among the neighboring nodes at the time of the deployment of the network. The authentication process includes sending a "Hello" message which is verified by the neighbor, and in response sends a "Response" message, to authenticate the node identity. Thus, tackling the threat of a WH attack. However, if a malicious node is present during the time of deployment, the key can be easily obtained by the attacker and invalidate this approach.

Qazi et al. [43] propose a protocol that is used to secure the Dynamic State Routing (DSR) protocol. In this approach, the round-trip time between the nodes is calculated and is compared with the data rate offered by IEEE 802.11g to verify if a WH exists in a network. The source node calculates the round-trip time of all the neighboring nodes involved in the route. Depending upon the time information that is received in the reply packet and the processing time, the node detects the Wormhole attack by comparing them with the data rate. If the difference between the expected and measured round trip time (RTT) is zero, then the network is secure from the Wormhole attack. However, if the difference is greater than zero, the Wormhole attack is said to exist. Its advantage lies in the fact that it can be implemented for both, multi-rate transmission as well as fixed-rate transmission. However, this process requires additional memory to store the RTT data, and it has additional computational requirements for measuring the RTT.

Bendjima et al. [44] propose a technique that couples the WH link detection algorithm and reorganization of the network based on the use of sectors and mobile agents. The main objective is to strengthen the creation of highly reliable and secure routes. The Mobile Agents are circulated through a sector which aggregates the collected data from the nodes and jointly transfers them as a joint unit. During the deployment phase, keys are shared between all the nodes. When the sectors are drawn in the network, keys are exchanged by the BS within each sector. The Mobile Agent itinerary is drawn with an optimal path. On receiving the Mobile Agent, the sink verifies the source of data. If the source node is found in the list of the assumed malicious nodes which have been formulated on the basis of the location of the nodes, then the sink advertises the identity of the node to the entire network. However, this approach is not effective against the simultaneous vulnerabilities that accompany the WH attack. There is an increased utilization of energy and packet data loss during the attack that was observed during the simulations.

Sharma et al. [45] postulate that the routing protocols such as AODV do not have a node capability check before updating the routing table, therefore making it easy to introduce a high transmission power node in the routing table. To mitigate this threat, a modified AODV is introduced with a capability check that helps in blacklisting an unlimited number of malicious nodes. However, the initial capability checks increase the delay, and additionally, jitters have also been observed. The WH Resistant Hybrid Technique (WRHT) has been proposed by Singh et al. [46]. It combines the use of Watchdog algorithm and the Delphi method to detect the presence of a WH attack. WHRT is considered as an offshoot of the AODV routing protocol. During the route discovery phase of AODV, time delay probability per-hop (TDPH) is calculated, and thus, time delay probability for the complete path is measured. The TDPH is measured to further calculate time delay probability (TDPP) for the complete path. Then packet loss probability per hop is calculated to determine the packet loss probability for the complete path. These values are used to determine if a Wormhole link exists or not. This approach has been found highly effective against Wormhole attack with better detection accuracy. However, its effectiveness against multiple wormhole channels is not established. Additionally, it requires complex calculations.

Amish et al. [47] presented a modified version of the AODV protocol for detecting multiple paths existing between two nodes, named as, Ad-Hoc On-Demand Multipath Distance Vector (AOMDV) routing protocol. The data sending nodes send a request (RREQ) packet to the destination node via a known path registered in the routing table. In case of an absence of a route, the sender nodes broadcast the RREQ packet. In response to the RREQ packet, the sender via multiple paths existing between the two communicating nodes receives a response (RREP) packet. For the detection of the malicious path or the Wormhole tunnel, the sender node calculates the round-trip time (RTT) of each path from which it receives the RREP packet. Using the average RTT and hop counts of each path, a threshold RTT is computed. If the RTT of a path is less than the threshold value and the number of hops is two, the path is declared as a WH. The next step involves removing the malicious nodes from the routing paths. This method can be applied in mobile WSN's like H-IoT but suffers from a large computational overhead.

Shukla et al. [48] present an IDS based on machine learning called ML-IDS. It combines three machine learning (ML) based approaches tailored for RPL based IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN). The first approach is called KM-IDS, which is K-means based clustering algorithm. The network is divided into 'K' clusters or safe zones. The value of K should be optimal and is calculated by using distortion cost

function and Elbow Method sequentially. Each safe zone has a centroid that connects the cluster to the gateway that is denoted as 6BR. Nodes are assigned to each cluster based on their physical co-ordinates. Within each cluster, the centroid is moved in 30 iterations to determine the optimal centroid position and hence, an optimal safe zone. The KM-IDS detects a WH when a node from another safe zone requests neighborhood status.

In the second approach called DT-IDS, which is based on the decision trees (DT), the DT is initially trained with a given network topology. The training helps in determining the threshold distance for establishing neighborhood. This threshold distance is the maximum permissible distance between any two directly connected neighbors. If a node sends a neighborhood request from a distance greater than the threshold, the request is denied and classified as malicious. Additionally, a network can be trained by a topology, which is similar in distribution; else the optimum threshold distance cannot be determined.

The third approach is the hybrid approach, which combines the clustering from the KM-IDS and threshold formulation from the DT-IDS. The request to add a neighbor from another safe zone is granted, only if the requesting node is within the threshold distance. The accuracy found using these three approaches is significant, taking into account that this is one of the first ML-based approaches. The limitations of this approach are based on finding the optimal K as well as distance values. The number of false positives is high if the K value is large, and the detection rate is low if the K value is small. The hybrid approach tries to make a tradeoff between the two. However, the detection accuracy is comparatively low. Furthermore, such calculations require significant power resources, which are essentially limited in H-IoT nodes.

Ahsan et al. [49] propose two approaches for Wormhole detection in RPL networks. In the case of a failure of one approach, the alternative provides the backup. This approach uses the Area Border Router (ABR) and the Sensing Aware Nodes (SANs) for detection. Both the techniques calculate the received signal strength (RSS). The ABR is a sink that connects the nodes to the internet. It provides a bi-directional link for establishing Point to Multi-Point (P2MP) and Multi-Point to Point (MP2P) connections. It has a neighborhood radius set at a default 100 m. When a node requests to be added as a neighbor, its RSS is calculated and converted into distance. If it exceeds the safe limit, the attack alert is raised. The IDs of all the nodes are verified, and the nodes having malicious nodes in the neighborhood tables are warned to remove the malicious nodes from their neighborhood tables.

The second approach uses sensing aware nodes to detect WH links. The SANs are special nodes having the capability to identify their geographical location. Before the network is initialized, the SANs broadcast a message. The nodes in the region reply with their IDs. If the IDs are incorrect, the nodes are rejected. After initialization, if a node from the region of another SAN requests to be added as a neighbor, the prospecting SAN requests the details of this node from the current SAN to authenticate its credentials. The second step involves calculating the RSS for determining the distance of the requesting node from the SAN. If it exceeds the default radius, the request is rejected, and a notification will be raised. The normal neighbors also contribute to the authentication process by checking the neighborhood tables after fixed intervals and authenticating the neighboring nodes using the RSS values. In case of discrepancies, the ABR and SANs are notified. This method provides enhanced security against the Wormhole attack by providing alternates in case one method fails. However, this method is not suitable for H-IoT applications as the SANs are specialized nodes that need positioning systems and enhanced capabilities to calculate the RSS. This is an immensely complex system that requires calculating power that is limited for H-IoT devices.

Rmyati et al. [50] present a graph-based method for the detection of WH attack specialized for Mobile Ad-hoc Networks (MANETs). The essential principle behind its working is that a WH tunnel reduces the length of the path between two nodes significantly. The proposed method utilizes the routing information enclosed by the transmitted messages. The method analyzes the received RREQ messages to determine the number of hops in the path between two communicating nodes. When an intermediary node receives an RREQ packet, it looks up its routing table to check for existing routes. In case the entry is already in the table, it updates its neighborhood relation information containing next-hop and number of hops. The graph is thus constructed, and the distances are calculated for the routes from source to destination. The nodes with the shortest path are grouped as suspected nodes. A link is termed as WH when the ratio between the length of the shortest path through the neighbors and the shortest path through the suspect nodes is greater than the detection threshold value. This method does not require any special positioning tools or clock synchronization. The accuracy of this method is based on the accuracy of the threshold value. The threshold value determines the number of false positives. Furthermore, the detection rate is better for longer values of the WH tunnel. For smaller values, the accuracy is not up to the mark but for hop length greater than five nodes; the detection accuracy is 100%. This method, however, increases the end-to-end delay (ETE).

Tables 2 and 3 present the summary of the counter-measures used against the SF and WH attacks, respectively. The tables highlight the significance and limitations of the currently deployed counter-measures.

Table 2 Counter-measures against selective forwarding attack and their limitations

References	Key concept	Significance	Limitations
[31]	Reputation Table based method to detect and eliminate Selective Grayhole attack (SGHA)	Can detect SGHA that usually confuse other approaches	Computationally and resource intensive approach
		Improves data delivery rate near the gateway node	Additional memory requirements for table maintenance
[33]	Attack detection using three types of control packets, Report, Acknowledgment and Alarm packets	Upstream and downstream detection processes are varied	Is prone to increased calculation and overhead
			False alarms are generated which need to be verified by the source node or BS
			Large delay incurred
[34]	Attack detection and data recovery using Per-Hop Acknowledgment (PHACK)	High detection accuracy	Not effective for mobile IoT
		Lost data recovery	Poor energy efficiency at the periphery
[35]	Implemented a modified AODV protocol	Can detect and mitigate single as well as collaborative Selective Forwarding attack	Has been tested for a small network only
			Nodes away from the BS face high latency
			Not suitable for a large network
[36]	CSR-A methodology implemented to detect the Selective Forwarding attack	Improves packet delivery ratio by approx. 10%.	High computational overhead
		Can be implemented along with any routing protocol	Storage requirements for reputation table
[37]	Sequential Probability Ratio Test (SPRT) and adaptive threshold of acceptable probability of dropped packets-based methodology	Suited to mobile networks using IPv6 based RPL protocol	High overhead involved
		High detection rate	Network congestion due to large number of 'Hello' packets
[38]	Anomaly-based Intrusion Detection System called mIDS	Less overhead as parameters are locally evaluated	False alarms affect the performance
	Uses Binary Logistic Regression (BLR) for classification	Offline evaluation	
[39]	Extended Data Routing Information (EDRI) based approach for MANETs	Used for detection of Blackhole attack, a subset of SF attack	High overhead caused due to use of additional control packets
		Suitable for collaborating nodes and detection of multiple malicious nodes	Increased network traffic
			Delay increased
[40]	Attack detection using a three-tier solution.	Can recover lost packets	Additional computational overhead
	Composed of SCAD, timeout and hop by hop mechanism		Not suitable for active detection when multiple nodes are colluding
[41]	Three tier approach, detection of malicious, securing the data using ECC & packet validation and secure routing using CS algorithm	High performance and energy efficiency	Latency not optimized for H-IoT

4 Proposed framework for mitigating SF and WH attacks

The majority of the current H-IoT systems follow a centralized model in which various nodes are identified, connected, and verified through a central node from cloud services with high data storage capabilities [51]. However, such kind of centralized model requires highly specialized and expensive infrastructure that impedes the large scale deployment of H-IoT systems. Another challenge associated with such network models is scalability, as the number of wearables is growing exponentially. This increased communication in the network leaves the network to become more vulnerable to security threats. Hence, securing the communication between the critical devices in an H-IoT system is becoming more complex.

Table 3 Counter-measures against wormhole attack and their limitations

References	Key concept	Significance	Limitations
[32]	Timing based approach	Reduced computational load	Failure to record timing renders process ineffective
		No requirement for synchronized clocks and one-to-one communication between the neighbors	
[42]	Uses a pre-shared key among the neighbouring nodes to verify the identity of the nodes	Highly effective in detecting the wormhole attacks	Not effective if the malicious node is present at the deployment stage
[43]	Based on calculation of the RTT and comparison with the system data rates of IEEE 801.11g	Protocol for securing the Dynamic State Routing (DSR) protocol	Additional computational requirements. Increased latency
[44]	Network partitioning into sectors using 'Mobile Agents'	Prevents the participation of malicious nodes in the routing table formulation	Increased energy consumption
			Increased packet drop ratio
[45]	Verifies the high capability nodes using hardware checks to keep malicious nodes out of routing tables	For mitigation process, End-To-End delay is improved	For normal process, ETE delay is increased
			Jitters are observed when mitigating the Wormhole attack
[46]	The Wormhole Resistant Hybrid Technique (WRHT) is implemented	Highly promising detection accuracy and can be used with any routing protocol	Effectiveness against multiple wormhole channels is not established
			High computational cost
[47]	Modified AODV protocol for multipath detection called AOMDV	Increased throughput	Additional computational overhead
[48]	Machine learning based IDS called ML-IDS	Tailored for RPL based 6LoWPAN	Need computational resources for complex calculations
	Three sub approaches, KM-IDS, DT-IDS and Hybrid IDS	Significant accuracy	Number of false alarms is significant
[49]	Area Border Router (ABR) and the Sensing Aware Nodes (SANs)	High accuracy	Requires specialized hardware for positioning
		Provides backup mechanism	Complex to implement
[50]	Graph Based Approach for MANETs	High accuracy with optimal values	The value of threshold requires careful selection. Process of selection not clear
		Requires no additional hardware	Increased End-to-End delay

Therefore, a decentralized approach is required to tackle such issues. Next, in this section, we briefly explain the blockchain technology and its potential advantages for H-IoT. At the end of the section, we propose a blockchain-based framework for mitigating SF and WH attacks in H-IoT.

4.1 Blockchain technology and its advantages for H-IoT

Blockchain technology is a distributed decentralized ledger that maintains data records and transactions (TX), where TXs are made by the nodes of the network and are recorded in the block [26]. The blocks are arranged in a time sequence and are assigned a timestamp, once added to the chain. The decentralized nature of blockchain does not require any central entity for administration. Moreover, blockchain technology is a cryptographic technology that is designed to ensure the prevention of data distortion and guarantee highly secure TXs. The blocks in the blockchain are hashed to their previous blocks, which means that a new block (possibly the malicious) cannot be substituted in between the blocks. Essentially, an extended block cannot be changed as well.

Today, blockchain integration into the IoT systems is rising [52]. A growing number of IoT-based industries are investing in blockchain technology. Therefore, one of the most interesting emerging trends is the potential integration of blockchain technology and H-IoT. A decentralized IoT network can provide blockchain technology with the ability to solve many of its security challenges, such as SF attack and the WH attack. The capabilities like decentralization, trustworthiness, autonomy, and scalability, make blockchain a potential complementing technology in the H-IoT ecosystems. For example, in the context of H-IoT security, blockchain can be used to ensure the secure and trustful

processing of critical TXs, the tracking of TXs, and the coordination of a large number of IoT-based smart devices. Another key importance is that blockchain technology can ensure the proper management of the health-related information at various levels. In addition to this, it records TXs in order, which means that the history of connected H-IoT devices can be recorded.

Owing to the fact that blockchain technology operates without the necessity of a centralized administrator, we see that integration possibilities and advantages are actually endless. There are three key benefits of using blockchain for H-IoT; building trust among the connected nodes, reduces costs, and accelerates transactions among the connected nodes [53]. By building trust between parties and devices, it reduces the risk of collusion and tampering. Blockchain technology reduces cost by removing overhead associated with intermediate nodes. It accelerates TXs between the connected nodes by reducing settlement time from days to near-instantaneous.

4.2 Blockchain-based framework for H-IoT security

In this section, we propose a blockchain-based framework for mitigating SF and WH attacks in an H-IoT environment. Our proposed framework suggests two scenarios for using blockchain technology to provide H-IoT network security (as shown in Fig. 5). In the first scenario, an H-IoT service provider integrates healthcare devices (sensors, wearables) to receive and transmit data and connects these devices to a blockchain network. At this point, blockchain technology provides the ability for the connected H-IoT devices to exchange messages, make orders, and complete TXs. The trustworthiness of the blockchain can mitigate the security attacks like SF and WH because these attacks use trust-less backdoors to attack the network. The client nodes (sensors) are connected to the gateway, which has sufficient energy and memory resources. Therefore, the gateway acts as an edge node. The blockchain is implemented at the edge node, which keeps the record of all the sensor nodes that join the network and who are authorized to send and receive data. If a malicious node tries to impersonate an authentic node, the blockchain is able to identify the malicious node. Additionally, all the sensor nodes keep track of the data traffic sent by them and update the gateway periodically. Since the gateway also knows the amount of data it receives from each client, it is able to detect any traffic pattern anomalies and also localize the source of the problem. The cloud also maintains a larger blockchain that implements the same principles for enhancing the scalability of the system. The stored data is processed using Big Data analytics to obtain a diagnosis for the user. Additionally, the analysis of the traffic flow from the gateway blockchain can help in real-time detection of SF and WH attacks.

The transparency in the blockchain makes it a suitable candidate for technology for enhancing the security of the network. In order to build trust between the nodes, the nodes connected with the gateway, share a pair of cryptographic keys. The keys are generated when a node is added to the network. Each of the transactions that they make, i.e., send or receive the data, is signed with their respective keys. The blockchain is implemented on the gateway that acts as an edge node. The gateway checks

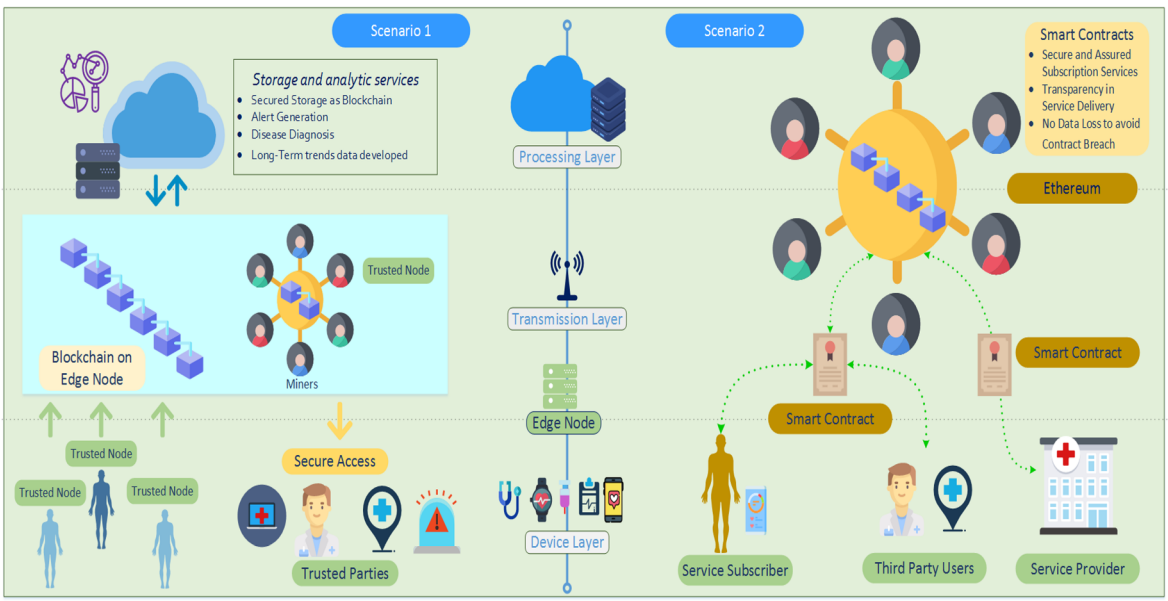

Fig. 5 The blockchain-based SF and WH attacks mitigation framework scenarios

each nodes' block for the cryptographic key. If the keys match, only then the block is allowed to be broadcasted in order to be approved by the miners. This authentication at the gateway can help in building trust in the nodes and avoid malicious nodes to take up false identities. Additionally, the malicious data from attackers can be prevented from being added to the database, thus protecting the integrity of the datasets. Algorithm 1 summarizes this approach.

Algorithm 1 Security mechanism framework in H-IoT using blockchain

Input: Public-keys of the sensor nodes, N_{ikeys}
Output: Secured datasets in a blockchain
Nodes joins the network. Gateway shares the unique keys with the nodes
The nodes upload the sensed data to the blockchain as a transaction block
If *The gateway authenticates the node key on the block,* $N_{ikeys} = N_{ikeys}(gateway)$ *is true*
BROADCAST the *Block* N_i
Add the *Block* N_i to the blockchain
Else (*DISCARD Block* N_i)
End If
End Procedure

In the second proposed scenario, Ethereum [54] smart contracts can be implemented into the H-IoT system in order to automate and regulate the healthcare services subscribed by the trustful nodes. Ethereum is a global, open-source blockchain platform for decentralized IoT applications, which provides the facility to write code that controls the digital information, runs as it is programmed and can be accessed from everywhere over the Internet. The reason we propose the use of Ethereum into the H-IoT framework for mitigating security issues is that it allows a seamless and safe exchange of TXs between connected nodes just as it performs in blockchain-based digital cryptocurrencies [55]. The services that are subscribed by the user are regulated by the terms and conditions of the smart contract, and if there are any violations of the terms and conditions, remedial actions can be automatically put into motion. The nodes in the blockchain subscribe to a service according to a smart contract. The wearables or nodes are identified using their unique keys. They enter in an agreement with the service provider to use the blockchain services provided by the Ethereum. The cryptographic-authentication of the nodes using the keys helps in securing the network from malicious nodes destabilizing the H-IoT. The Algorithm 2 illustrates the same.

Algorithm 2 Ethereum based security framework in H-IoT using blockchain

Input: Public-keys of the sensor nodes, N_{ikeys}, Linked Service Agreement (LSA)
Output: Secured transactions in a blockchain
Nodes enter in a smart contract when subscribing
The gateway authenticates the identity of the node and the LSA
If *The gateway authenticates the node identity and LSA*
ALLOW access to the blockchain
Else *IGNORE REQUEST* and report the malicious node
End If
End Procedure

4.2.1 Sample implementation scenario

Considering a WBAN based health monitoring system in a closed environment. The WBANs consist of a number of sensors connected to a gateway. A number of WBANs work collaboratively with each other to constitute a H-IoT. Figure 6 depicts this implementation scenario. The gateways, which are more capable than the other nodes participate in the blockchain. The gateways, which act as *miners* in the blockchain are able to verify a transaction by participating in a consensus algorithm [56]. The gateways are also able to create blocks and add to the blockchain after completing the consensus algorithm. The gateway nodes join the H-IoT and join the blockchain as *miners*.The Algorithm 1 is followed by the nodes to agree upon the identity of the nodes that try to add the data to the blockchain via the gateway that they are connected with. The use of consensus mechanism allows the participants in the blockchain to validate the authenticity of the block [57]. Since, the H-IoT system has a number of constraints in terms of resources, a lightweight mechanism proposed in [58] is followed for consensus. The *TrustChain* algorithm proposed is a permission-less and tamper-proof data structure that is used to store the transactions. The TrustChain is observed to be resistant to the *Sybil attack* [59]. The resistance against the Sybil attack allows a measurable defense against the 51% attack [60].

Additionally, the access to the blockchain can be governed by a LSA. In the structure as depicted in the Fig. 6, the gateways are able to access the blockchain via a set of rules defined in a smart contract, implemented using Ethereum. The Algorithm 2 governs the interaction between the gateway and the blockchain in this scenario.

5 Future research and recommendations

The limitations in the state-of-the-art counter-measures against the security threats in H-The methodologies discussed in Sect. 3 are insufficient for use in H-IoT due to

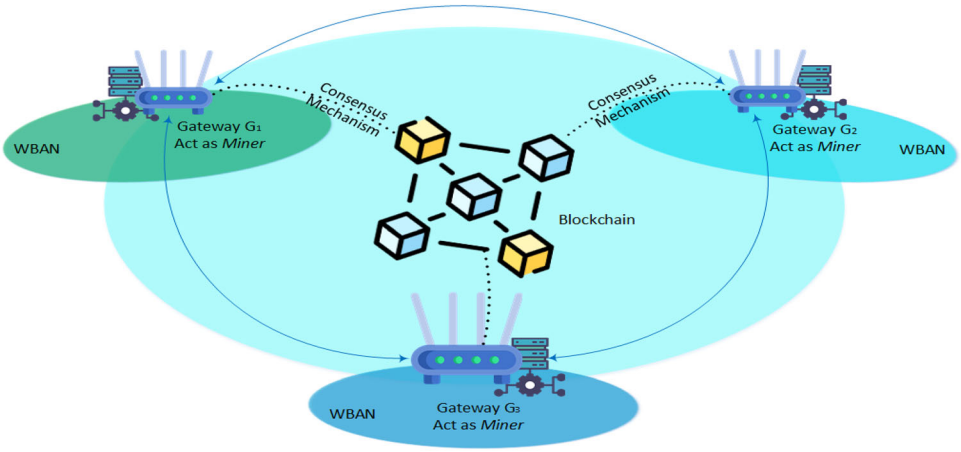

Fig. 6 Sample scenario for proposed implementation

several critical drawbacks. The essential features of H-IoT include low latency and low overhead. Therefore, we identify and highlight these flaws in the H-IoT. The limitations identified in the preceding sections open vast avenues for research in mitigating SF and WH attacks. We classify future research directions as follows,

1. *Scalability* The majority of current methodologies have limited effectiveness in large-scale networks. Since the H-IoT concept has been conceived for large-scale deployment, the current methods face issues like large delay and increased packet drops during packet transport. Large-scale IoT deployment requires maintenance of packet delivery ratio and negligible latency throughout the entire network. Methodologies based on distributed network controllers such as Software Defined Networks (SDNs) and Edge Computing can assist in alleviating this challenge.
2. *Computational overhead* The sensor nodes in the H-IoT are constrained in terms of power and energy. However, the current techniques incur a high computational cost, which requires computational and energy resources. Low computational methods take preference. Edge computing can play a definitive role in mitigating overhead constraints as the nodes can share the computational load with the edge devices. Low computational requirements also enhance energy efficiency.
3. *Active detection or real-time operation* As the security threats are becoming increasingly adaptable to current methods, the techniques for active detection of the attacks are required. Several colluding nodes may carry out orchestrated attacks, which are not detected by the traditional methods. Thus, an approach to counter such attacks is essential for better network security. Machine learning (ML) can contribute to the development of real-time detection methodologies. Additionally, H-IoT networks are highly dynamic. To differentiate between the malicious and genuine nodes in a changing environment, active attack detection, and localization techniques can be implemented. Artificial Intelligence-based approaches can trigger critical breakthroughs in this direction [61]. However, current ML algorithms are computationally complex. Therefore, low complexity and energy efficient ML algorithms are required.
4. *Energy efficiency* The WBAN nodes are designed for high energy efficiency, but the counter-measures against the network attacks require additional power. The energy efficiency remains the most critical challenge in the deployment of H-IoT systems. Energy-efficient sensor designs and alternative novel power sources can be explored to enhance the energy efficiency of the nodes [62]. The use of energy harvesting from the human body can be explored [63]. The implantable sensors can utilize the body heat for fulfilling the energy requirements, therefore improving the lifetime of the overall system. The development of light-weight protocols can further improve energy efficiency without compromising the QoS of the system.
5. *Latency* The H-IoT is a time-critical system, and hence, the latency is required to be minimal. The need for low latency counter-measures is of paramount importance. The implementation of distributed architecture can effectively improve the delay-wise performance of the system. The fog/edge paradigm enables the implementation of security mechanisms that require higher computational capabilities in a decentralized scenario. The virtualization of network management functions using SDNs can be explored to implement security protocols without incurring an additional computational load on the resource-constrained nodes.
6. *Modern technologies* The effect of ML on various operational aspects of H-IoT is very profound. The contribution of ML as an enabling technology for

underlying processes as well as for data processing is immense. ML is being used for securing the data and network information. Intrusion detection systems (IDSs) based on the ML algorithms are highly efficient, but they require computational power, which is scarce in H-IoT nodes. Therefore, RL methods can be explored for the implementation of security systems in H-IoT scenario. The introduction of ML especially the Reinforcement Learning (RL) techniques can enhance the energy efficiency in mesh networks without incurring the computational overhead [64]. The use of AI-based solutions for ensuring the data delivery can be explored while considering multiple uncertainty introducing factors [65].

The use of distributed architectures can effectively improve the security of the system as the segments of the network can be analyzed thoroughly to detect any anomalies. The Fog/Edge computing enables the distributed design of an H-IoT network. The Fog/Edge nodes allow the implementation of security mechanisms that require higher computational capacities which are otherwise not available in an H-IoT system [66]. The immutable and transparent nature of the blockchains has allowed them to find their way in a diverse set of applications [67]. Blockchain involves a network of nodes that can view all the information and therefore maintain trust and security by scrutinizing the data that is added to the blockchain. Blockchains can be used for maintaining the record of the sensor in the network, their contribution to the data sets and building trust among the participating nodes. Taking into consideration the issues mentioned above, we can additionally explore the areas like cryptographic verification techniques for neighborhood sensing. Trust-based approaches can enhance the security of data shared between the neighboring nodes [68].

6 Conclusion

The H-IoT constitutes a system of sensors that monitor the physio-chemical data generated by the physiological processes in the human body. The processed data is used for generating the mathematical models for the detection of anomalies and detecting any emergencies. The transmitted data is highly sensitive and demands immunity from unauthorized modifications. This paper presents the characteristics of the Selective Forwarding (SF) and Wormhole (WH) attacks in IoT systems which cause an information deficit in the network. A variety of approaches have been adopted by to protect this sensitive data from being accessed and modified without authorization. A number of diverse counter-measures are reviewed to highlight their significance and limitations. These counter measures use a diverse methodologies, including modifying network layer protocols, modifying control data, implementing ML. The limitations of the state-of-the-art counter-measures are highlighted. These drawbacks are studied to generate a blockchain based security model. In addition, we propose a framework to exploit the features of blockchain for mitigating these security issues in H-IoT systems. Proposed framework suggests using two scenarios for the implementation of blockchain for security in H-IoT. Finally, we outline a number of future research directions aimed at improving the security of the H-IoT systems against SF and WH attacks.

As future work, we aim to implement our proposed framework for mitigating trust-based security issues in H-IoT. Moreover, the requirements of H-IoT remain very critical of latency and data integrity; hence, a guarantee of these features remains of utmost importance. Therefore, we also aim to explore the proposed framework from the point of view of these key requirements.

Acknowledgements This research was supported in part by the Brain Korea 21 Plus Program (Grant No. 22A20130012814) funded by the National Research Foundation of Korea (NRF), in part by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (Grant No. IITP-2019-2016-0-00313) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation), and in part by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. 2018R1D1A1A09082266).

References

1. Alagar, V., Alsaig, A., Ormandjiva, O., Wan, K.: Context-based security and privacy for healthcare IoT. In: 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), Xi'an, pp. 122–128 (2018). https://doi.org/10.1109/SmartIoT.2018.00-14
2. Ramli, S.N., Ahmad, R.: Surveying the wireless body area network in the realm of wireless communication. In: 2011 7th International Conference Information Assurance and Security (IAS), Melaka, pp. 58–61 (2011). https://doi.org/10.1109/ISIAS.2011.6122845
3. Suresh, P., Daniel, J.V., Parthasarathy, V., Aswathy, R.H.: A state of the art review on the Internet of Things (IoT) History, Technology and fields of deployment. In: 2014 International Conference on Science Engineering and Management (ICSEMR), Chennai, India, pp. 1–8 (2014). https://doi.org/10.1109/ICSEMR.2014.7043637
4. Qadri, Y.A., Musaddiq, A., Kim, D.W., Kim, S.W.: An overview of selective forwarding and wormhole attacks in healthcare IoT. In: Asia Pacific Conference on Information Communication Technology (APCICT-2018), Daegu, Korea (2018)
5. Naik, M.R.K., Samundiswary, P.: Wireless body area network security issues-survey. In: 2016 International Conference on Control, Instrumentation, Communication and Computational

Technologies (ICCICCT), Kumaracoil, India, pp. 190–194 (2016). https://doi.org/10.1109/ICCICCT.2016.7987943
6. He, D., Zeadally, S., Kumar, N., Lee, J.H.: Anonymous authentication for wireless body area networks with provable security. IEEE Syst. J. **11**(4), 1–12 (2017). https://doi.org/10.1109/JSYST.2016.2544805
7. Lin, Y.-J., Chen, H.-S., Su, M.-J.: A cloud based bluetooth low energy tracking system for dementia patients. In: 2015 Eighth International Conference on Mobile Computing and Ubiquitous Networking (ICMU), Hakodate, pp. 88–89 (2015). https://doi.org/10.1109/ICMU.2015.7061043
8. IEEE Standard for Low-Rate Wireless Networks. IEEE Std 802.15.4-2015 (Revision of IEEE Std 802.15.4-2011), pp. 1–709, (2016). https://doi.org/10.1109/IEEESTD.2016.7460875
9. Ali, R., Kim, S.W., Kim, B., Park, Y.: Design of MAC layer resource allocation schemes for IEEE 802.11ax: future directions. IETE Tech. Rev. **35**(1), 28–52 (2018). https://doi.org/10.1080/02564602.2016.1242387
10. He, S., Cheng, B., Wang, H., Huang, Y., Chen, J.: Proactive personalized services through fog-cloud computing in large-scale iot-based healthcare application. China Commun. **14**(11), 1–16 (2017). https://doi.org/10.1109/CC.2017.8233646
11. Ridhawi, I.A., Aloqaily, M., Kotb, Y., Jararweh, Y.: A profitable and energy-efficient cooperative fog solution for IoT services. In: IEEE Transactions on Industrial Informatics (Early Access) (2019). https://doi.org/10.1109/TII.2019.2922699
12. Buyukakkaslar, M.T., Erturk, M.A., Aydin, M.A., Vollero, L.: LoRaWAN as an e-health communication technology. In: 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, pp. 310–313 (2017). https://doi.org/10.1109/COMPSAC.2017.162
13. Lavric, A., Petrariu, A.I., Popa, V.: Long range sigfox communication protocol scalability analysis under large-scale, high-density conditions. IEEE Access **7**, 35816–35825 (2019). https://doi.org/10.1109/ACCESS.2019.2903157
14. Anand, S, Routray, S.K.: Issues and challenges in healthcare narrowband IoT. In: 2017 international conference on inventive communication and computational technologies (ICICCT), Coimbatore, pp. 486–489 (2017). https://doi.org/10.1109/ICICCT.2017.7975247
15. Baker, S.B., Xiang, W., Atkinson, I.: Internet of things for smart healthcare: technologies, challenges, and opportunities. IEEE Access **5**, 26521–26543 (2017). https://doi.org/10.1109/ACCESS.2017.2775180
16. Zafar, S., Jangsher, S., Bouachir, O., Aloqaily, M., Othman, J.B.: QoS enhancement with deep learning-based interference prediction in mobile IoT. Comput. Commun. **148**, 86–97 (2019). https://doi.org/10.1016/j.comcom.2019.09.010
17. Firouzi, F., Farahani, B., Ibrahim, M., Chakrabarty, K.: From EDA to IoT eHealth: promise, challenges, and solutions. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **37**(12), 1–16 (2018). https://doi.org/10.1109/TCAD.2018.2801227
18. Faheem, M., Gungor, V.C.: Capacity and spectrum-aware communication framework for wireless sensor network-based smart grid applications. Comput. Stand. Interfaces **53**, 48–58 (2017). https://doi.org/10.1016/j.csi.2017.03.003
19. Faheem, M., Butt, R.A, Raza, B, Ashraf, M.W, Begum, S, Ngadi, M.A, Gungor, V.C: Bio-inspired routing protocol for WSN-based smart grid applications in the context of Industry 4.0. In: Transactions on Emerging Telecommunications Technologies (2018). https://doi.org/10.1002/ett.3503
20. Faheem, M., Gungor, V.C.: Energy efficient and QoS-aware routing protocol for wireless sensor network-based smart grid applications in the context of industry 4.0. Appl. Soft Comput. **68**, 910–922 (2018). https://doi.org/10.1016/j.asoc.2017.07.045
21. Faheem, M., Abbas, M.Z., Tuna, G., Gungor, V.C.: EDHRP: Energy efficient event driven hybrid routing protocol for densely deployed wireless sensor networks. J. Netw. Comput. Appl. **58**, 309–326 (2015). https://doi.org/10.1016/j.jnca.2015.08.002
22. Al-Turjman, F., Ever, E., Zahmatkesh, H.: Internet of nano-things (IoNT) & WBAN. In: Al-Turjman, F. (ed.) Internet of Nano-Things and Wireless Body Area Networks (WBAN). CRC Press, Baco Raton (2019)
23. Topel, S.D., Al-Turjman, F.: Nanosensors for the internet of nano-things (IoNT): an overview. In: Al-Turjman, F. (ed.) Internet of Nano-Things and Wireless Body Area Networks (WBAN). CRC Press, Boca Raton (2019)
24. Balasubramanian, V., Zaman, F., Aloqaily, M., Ridhawi, I.A., Jararweh, Y., Salameh, H.B.: A mobility management architecture for seamless delivery of 5G-IoT services. In: 2019 IEEE International Conference on Communications (ICC 2019), Shanghai, China, pp. 1–7 (2019). https://doi.org/10.1109/ICC.2019.8761658
25. Tomić, I., McCann, J.A.: A survey of potential security issues in existing wireless sensor network protocols. IEEE Internet Things J. **4**(6), 1910–1923 (2017). https://doi.org/10.1109/JIOT.2017.2749883
26. Zheng, Z., Xie, S., Dai, H.-N., Wang, H.: Blockchain challenges and opportunities: a survey. Int. J. Web Grid Serv. **14**, 352–375 (2016). https://doi.org/10.1504/ijwgs.2018.10016848
27. Dwivedi, A.D., Srivastava, G., Dhar, S., Singh, R.: A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **19**(2), 326 (2019). https://doi.org/10.3390/s19020326
28. Salah, K., Rehman, M.H.U., Nizamuddin, N., Al-Fuqaha, A.: Blockchain for AI: review and open research challenges. IEEE Access **7**, 10127–10149 (2019). https://doi.org/10.1109/ACCESS.2018.2890507
29. Salleh, A., Mamat, K., Darus, M.Y.: Integration of wireless sensor network and web of things: security perspective. In: 2017 IEEE 8th Control and System Graduate Research Colloquium (ICSGRC), Shah Alam, Malaysia, pp. 138–143 (2017). https://doi.org/10.1109/ICSGRC.2017.8070583
30. Goyal, S., Bhatia, T., Verma, A.K.: Wormhole and Sybil attack in WSN: a review. In: 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp. 1463–1468 (2015)
31. Prabhakar, A., Anjali, T.: Mitigating selective Gray Hole Attack in wireless multi-hop network. In: 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, pp. 1223–1227 (2017). https://doi.org/10.1109/WiSPNET.2017.8299958
32. Khabbazian, M., Mercier, H., Bhargava, V.K.: Severity analysis and countermeasure for the wormhole attack in wireless ad hoc networks. IEEE Trans. Wireless Commun. **8**(2), 736–745 (2009). https://doi.org/10.1109/TWC.2009.070536
33. Yu, B., Xiao, B.: Detecting selective forwarding attacks in wireless sensor networks. In: 20th International Parallel and Distributed Processing Symposium (IPDPS), Rhodes Island, Greece (2006). https://doi.org/10.1109/IPDPS.2006.1639675
34. Liu, A., Dong, M., Ota, K., Long, J.: PHACK: an efficient scheme for selective forwarding attack detection in WSNs. Sensors **15**(12), 30942–30963 (2015). https://doi.org/10.3390/s151229835
35. Mathur, A., Newe, T., Rao, M.: Healthcare WSN: cluster elections and selective forwarding defense. In: NGMAST 9th International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, pp. 341–346 (2015). https://doi.org/10.1109/NGMAST.2015.14
36. Ren, J., Zhang, Y., Zhang, K., Shen, X.: Adaptive and channel-aware detection of selective forwarding attacks in wireless sensor

networks. IEEE Trans. Wireless Commun. **15**(5), 3718–3731 (2016). https://doi.org/10.1109/TWC.2016.2526601
37. Gara, F., Saad, L.B., Ayed, R.B.: An intrusion detection system for selective forwarding attack in IPv6-based mobile WSNs. In: 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, pp. 276–281 (2017). https://doi.org/10.1109/IWCMC.2017.7986299
38. Ioannou, C., Vassiliou, V., Sergiou, C.: An intrusion detection system for wireless sensor networks. In: 2017 24th International Conference on Telecommunications (ICT), Limassol, Cyprus, pp. 1–5 (2017). https://doi.org/10.1109/ICT.2017.7998271
39. Dorri, A.: An EDRI-based approach for detecting and eliminating cooperative black hole nodes in MANET. Springer Wirel. Netw. **23**(6), 1767–1778 (2017). https://doi.org/10.1007/s11276-016-1251-x
40. Pu, C., Lim, S.: A light-weight countermeasure to forwarding misbehavior in wireless sensor networks: design, analysis, and evaluation. IEEE Syst. J. **12**(1), 1–9 (2018). https://doi.org/10.1109/JSYST.2016.2535730
41. Mehetre, D.C., Roslin, S.E., Wagh, S.J.: Detection and prevention of black hole and selective forwarding attack in clustered wsn with active trust. Clust. Comput. **22**, 1313–1328 (2018). https://doi.org/10.1007/s10586-017-1622-9
42. Modirkhazeni, A., Aghamahamoodi, S., Modirkhazeni, A., Niknejad, N.: Distributed approach to mitigate wormhole attack in wireless sensor network. In: 7th International Conference on Networked Computing, Gyeongsanbuk-do, Korea, pp. 122–128 v
43. Qazi, S., Raad, R., Mu, Y., Susilo, W.: Securing DSR against wormhole attacks in multi-rate ad hoc networks. J. Netw. Comput. Appl. **36**(2), 582–592 (2013). https://doi.org/10.1016/j.jnca.2012.12.019
44. Bendjima, M., Feham, M.: Wormhole attack detection in wireless sensor networks. In: 2016 SAI Computing Conference (SAI), London, UK, pp. 1319–1326 (2016). https://doi.org/10.1109/SAI.2016.7556151
45. Sharma, M.K., Joshi, B.K.: A mitigation technique for high transmission power based wormhole attack in wireless sensor networks. In: 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, pp. 1–6 (2016). https://doi.org/10.1109/ICTBIG.2016.7892698
46. Singh, R., Singh, J., Singh, R.: WRHT: a hybrid technique for detection of wormhole attack in wireless sensor networks. J. Mob. Inf. Syst. **2016**, 1–13 (2016). https://doi.org/10.1155/2016/8354930
47. Parmar, A., Vaghelab, V.B.: Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol. Procedia Comput. Sci. **79**, 700–707 (2016). https://doi.org/10.1016/j.procs.2016.03.092
48. Shukla, P.: ML-IDS: A machine learning approach to detect Wormhole attacks in Internet of Things. In: 2017 Intelligent Systems Conference (IntelliSys), London, pp. 234–240 (2017). https://doi.org/10.1109/IntelliSys.2017.8324298
49. Ahsan, M.S., Bhutta, M.N.M., Maqsood, M.: Wormhole attack detection in routing protocol for low power lossy networks. In: 2017 International Conference on Information and Communication Technologies (ICICT), Karachi, pp. 58–67 (2017). https://doi.org/10.1109/ICICT.2017.8320165
50. Rmayti, M., Begriche, Y., Khatoun, R., Khoukhi, L., Mammeri, A.: Graph-based wormhole attack detection in mobile ad hoc networks (MANETs). In: 2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ), Florida, USA, pp. 1–6 (2018). https://doi.org/10.1109/MOBISECSERV.2018.8311439
51. Zikria, Y.B., Kim, S.W., Hahm, O., Afzal, M.K., Aalsalem, M.Y.: Internet of Things (IoT) operating systems management: opportunities, challenges, and solution. Sensors **19**(8), 1–10 (2019). https://doi.org/10.3390/s19081793
52. Reyna, A., Martín, C., Chen, J., Soler, E., Díaz, M.: On blockchain and its integration with IoT: challenges and opportunities. Future Gener. Comput. Syst. **88**, 173–190 (2018). https://doi.org/10.1016/j.future.2018.05.046
53. Huh, S., Cho, S., Kim, S.: Managing IoT devices using blockchain platform. In: 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, pp. 464–467 (2017). https://doi.org/10.23919/ICACT.2017.7890132
54. Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N.: A survey on privacy protection in blockchain system. J. Netw. Comput. Appl. **126**, 45–58 (2019). https://doi.org/10.1016/j.jnca.2018.10.020
55. Antonopoulos, A.M.: Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 1st edn. O'Reilly Media, Inc., Newton (2014). ISBN:1449374042 9781449374044
56. Virmani, C., Gupta, D.J., Choudhary, T.: Blockchain 2.0: an edge over technologies. In: Architectures and Frameworks for Developing and Applying Blockchain Technology. IGI Global, Pennsylvania (2019). https://doi.org/10.4018/978-1-5225-9257-0.ch009
57. Monrat, A.A., Schelén, O., Andersson, K.: A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access **7**, 117134–117151 (2019). https://doi.org/10.1109/ACCESS.2019.2936094
58. Otte, P., Vos, N.D., Pouwelse, J: TrustChain: A Sybil-resistant scalable blockchain. Future Gener. Comput. Syst. (2017). https://doi.org/10.1016/j.future.2017.08.048
59. Douceur, J.R.: The sybil attack. In: 1st International Workshop on Peer-To-Peer Systems (IPTPS), Berlin, pp. 251–260 (2002)
60. Sayeed, S., Marco-Gisbert, H.: Assessing blockchain consensus and security mechanisms against the 51% attack. Appl. Sci. **9**(9), 1788 (2019). https://doi.org/10.3390/app9091788
61. Aloqaily, M., Otoum, S., Al Ridhawi, I., Jararweh, Y.: An intrusion detection system for connected vehicles in smart cities. Ad Hoc Netw. **90**, 101842 (2019). https://doi.org/10.1016/j.adhoc.2019.02.001
62. Al-Turjman, F., Din, S., Paul, A.: Energy monitoring in IoT-based ad hoc networks: an overview. Comput. Electr. Eng. **76**, 133–142 (2019). https://doi.org/10.1016/j.compeleceng.2019.03.013
63. Demir, S.M., Al-Turjman, F., Muhtaroglu, A.: Energy-harvesting methods for WBAN applications. In: Al-Turjman, F. (ed.) Internet of Nano-Things and Wireless Body Area Networks (WBAN). CRC Press, Boca Raton (2019)
64. Balasubramanian, V., Zaman, F., Aloqaily, M., Alrabaee, S., Gorlatova, M., Reisslein, M.: Reinforcing the edge: autonomous energy management for mobile device clouds. In: IEEE International Conference on Computer Communications, Paris, France (2019)
65. Al-Turjman, F., Zahmatkesh, H., Mostarda, L.: Quantifying uncertainty in internet of medical things and big-data services using intelligence and deep learning. In: IEEE Access (Early Access). https://doi.org/10.1109/ACCESS.2019.2931637
66. Balasubramaniam, V., Aloqaily, M., Zaman, F., Jararweh, Y.: Exploring computing at the edge: a multi-interface system architecture enabled mobile device cloud. In: 2018 IEEE 7th International Conference on Cloud Networking (CloudNet),Tokyo, Japan (2018). https://doi.org/10.1109/CloudNet.2018.8549296
67. Dai, Y., Xu, D., Maharjan, S., Chen, Z., He, Q., Zhang, Y.: Blockchain and deep reinforcement learning empowered intelligent 5G beyond. IEEE Netw. **33**, 10–17 (2019). https://doi.org/10.1109/MNET.2019.1800376

68. Rathee, G., Sharma, A., Iqbal, R., Aloqaily, M., Jaglan, N., Kumar, R.: A blockchain framework for securing connected and autonomous vehicles. Sensors **19**, 3165 (2019). https://doi.org/10.3390/s19143165

Yazdan Ahmad Qadri received his Master's and Bachelor's degree in electronics and communication engineering from L.P. University, India. He completed his M. Tech program in 2016 with a focus on digital signal processing. He is currently pursuing his Ph.D. from the Department of Information and Communication Engineering, Yeungnam University, South Korea. His research targets Medicine 4.0 enabling technologies encompassing IoT, AI, Edge Computing and SDN.

Rashid Ali (Ph.D.) received his B.S. degree in Information Technology from Gomal University, Pakistan in 2007 and his M.S. degree under supervision of Dr. Stanislav Belenki in Computer Science (Advanced Network Design) in 2010 and M.S. degree in Informatics under the supervision of Dr. Maria Spante in 2012–2013 from the University West, Sweden. He received his Ph.D. diploma in Information and Communication Engineering from the Department of Information and Communication Engineering, Yeungnam University, Korea in February 2019. Between 2007 and 2009, he worked for Wateen Telecom Pvt. Ltd. Pakistan as WiMAX Engineer in Operations & Research Department. From July 2013 to June 2014, he worked for COMSATS University (Vehari), Pakistan, as a Lecturer. Currently, he is working as a PostDoc researcher at the School of Intelligent Mechatronics Engineering, Sejong University Seoul, Korea. His research interests include next-generation wireless local area networks (IEEE 802.11ax/ah), unlicensed wireless networks in 5G, Internet of Things, performance evaluation of wireless networks, Named-Data/Information-Centric Networking, Deep Learning techniques for wireless networks, and Blockchain technology for IoT trustworthiness.

Arslan Musaddiq received his M.S. degree in communication and network engineering from University Putra Malaysia (UPM) in 2015 and obtained his B.S. in electrical engineering (telecommunication) from Bahria University, Islamabad, Pakistan in 2011. He is currently a PhD student in the Department of Information and Communication Engineering, Yeungnam University, Gyeongsan-Si, South Korea. His research interests are primarily in the areas of wireless networking, Internet of Things, wireless resource management, routing protocols and ad hoc networks.

Fadi Al-Turjman received his Ph.D. in computer science from Queen's University, Kingston, Ontario, Canada, in 2011. He is a professor at Artificial Intelligence Department, Near East University, Nicosia, Mersin, Turkey. Professor Al-Turjman is a leading authority in the areas of smart/cognitive, wireless, and mobile networks' architectures, protocols, deployments, and performance evaluation. His publication history spans over 200 publications in journals, conferences, patents, books, and book chapters, in addition to numerous keynotes and plenary talks at flagship venues. He has written and edited more than fifteen books about cognition, security, and wireless sensor networks' deployments in smart environments, published by Taylor & Francis and Springer. He has received several recognitions and best papers' awards at top international conferences. He also received the prestigious Best Research Paper Award from Elsevier Computer Communications Journal for the period 2015–2018, in addition to the Top Researcher Award for 2018 at Antalya Bilim University, Turkey. Professor Al-Turjman has led a number of international symposia and workshops in flagship communication society conferences. Currently, he serves as the lead guest editor for several well reputed journals, including the Elsevier Computer Communications and the IET Wireless Sensor Systems journals.

Dae Wan Kim is a Professor at School of Business, Yeungnam University in Korea. He received his PhD in Information Systems from London School of Economics (LSE) in the UK. His current research interests include digital business, social media, and mobile cloud computing.

Sung Won Kim received his B.S. and M.S. degrees from the Department of Control and Instrumentation Engineering, Seoul National University, Korea, in 1990 and 1992, respectively, and his Ph.D. degree from the School of Electrical Engineering and Computer Sciences, Seoul National University, Korea, in August 2002. From January 1992 to August 2001, he was a Researcher at the Research and Development Center of LG Electronics, Korea. From August 2001 to August 2003, he was a Researcher at the Research and Development Center of AL Tech, Korea. From August 2003 to February 2005, he was a Postdoctoral Researcher in the Department of Electrical and Computer Engineering, University of Florida, Gainesville, USA. In March 2005, he joined the Department of Information and Communication Engineering, Yeungnam University, Gyeongsangbuk-do, Korea, where he is currently a Professor. His research interests include resource management, wireless networks, mobile computing, performance evaluation, and machine learning.