IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received March 19, 2020, accepted April 2, 2020, date of publication April 6, 2020, date of current version April 22, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2985851

RTS: A Robust and Trusted Scheme for IoT-Based Mobile Wireless Mesh Networks

KHALID HASEEB[1], IKRAM UD DIN[2], (Senior Member, IEEE), AHMAD ALMOGREN[3], (Senior Member, IEEE), NAVEED ISLAM[1], AND AYMAN ALTAMEEM[4]

[1]Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Pakistan
[2]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan
[3]Chair of Cyber Security, Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia
[4]Department of Natural and Engineering Sciences, College of Applied Studies and Community Services, King Saud University, Riyadh 11543, Saudi Arabia

Corresponding author: Ahmad Almogren (ahalmogren@ksu.edu.sa)

This work was supported by the Deanship of Scientific Research, King Saud University, through the Vice Deanship of Scientific Research Chairs.

ABSTRACT Wireless mesh networks consist of various mesh clients that are organized in an unfixed infrastructure and packets are forwarded using a multi-hop model. Routing protocols have a significant impact on mesh networks because their performance has a crucial effect on nodes connectivity and throughput. Recently, the integration of mesh clients with the Internet of Things (IoT) has gained significant importance to connect billions of machines and achieve fast coverage with minimum network cost. However, if mesh clients are mobile, then data routing via intermediate nodes gives a noteworthy effect on the network performance and latency. Furthermore, over the Internet, a malicious node may be a part of the mesh network and as a result, the sending information can be manipulated and compromised. Therefore, this research article aims to propose a robust and trusted scheme (RTS) for IoT-based mobile mesh networks to provide reliable routing, data confidentiality, and integrity. Firstly, the proposed scheme presents a robust data routing among mobile mesh clients, routers and gateway devices based on the network parameters and measurement of wireless channels. Moreover, the wireless channels between mesh devices are formulated based on the efficacy of link costs for data dissemination. Besides, the location of mobile mesh clients is determined by computing the distance vector at a regular time interval. Secondly, a secure and authentic data protection technique is proposed using public-private key cryptography, which aims to increase the protection of mesh clients with minimal overhead. The competence of the proposed scheme is significantly improved with respect to network throughput by an average of 14%, packet loss rate by an average of 37%, latency rate by an average of 12%, computational overhead by an average of 34%, and energy efficiency by an average of 20% as compared to other works.

INDEX TERMS Wireless mesh network, the Internet of Things, data security, gateways, routing protocol.

I. INTRODUCTION

In the past two decades, the technology of wireless networks played a crucial role in the development of different network domains [1]–[4]. It interconnects a huge number of wireless nodes by using wireless links to capture information and transfer it towards end-points. Intermediate devices called next-hops are used as data forwarders and transmit the information in a multi-hop manner [5]–[7]. Users can obtain the required information through servers over the Internet. Wireless mesh networks are also called wireless ad-hoc network and consist of a huge number of mesh clients, mesh routers, and gateway devices to cover a large region for information gathering and forwarding.

In the architecture of wireless mesh networks [8]–[11], each node receives the information and forwards it to its neighbor to perform data routing. Routing schemes can be categorized into static and mobile methods. In the static method, wireless nodes are fixed and after the network deployment, they cannot change their positions. While the nodes that are shifting their positions after the deployment fall in mobile networks. Mobile nodes give better coverage as

The associate editor coordinating the review of this manuscript and approving it for publication was Min Xia.

compared to static nodes, however, the optimal route selection and secure data forwarding are most of the important research challenges [12]–[14].

The architecture of the Internet of Things (IoT) connects all communication devices, i.e., static or mobile, for the environment monitoring and leads to the development in various network fields [4], [15]–[17]. IoT does not connect traditional devices, e.g., laptops and cell phones, for data communications but also physical objects like cars, fans, watches, and other smart devices. Furthermore, due to the dynamic nature of wireless mesh networks, these bring a significant impact on IoT-based applications especially the network adaptability and coverage with improved connectivity [18]–[20]. Nowadays, different applications such as smart cities, smart health, and smart agriculture are integrated mesh clients with IoT devices for data collection, which are forwarded to the central station [21]–[23]. The main benefit of using wireless mesh networks is to add or replace a mesh client in the existing IoT-based network without disturbing the rest of the mesh clients. Also, most of the applications that are developed with the integration of wireless mesh clients and IoT devices are heterogeneous for algorithms, coverage, delivery performance, etc.

Wireless mesh networks provide the features of both traditional wireless and mobile ad-hoc networks. Therefore, the field of a wireless mesh network is gaining a lot of attention in both industrial and academic domains [24]–[26]. As compared to mobile ad-hoc networks, most of the mesh clients have a limited movement and are deployed randomly. Mesh clients can be connected or disconnected to a network structure at any time without any disruption. All mesh clients communicate through routers that are joined to the virtual backbone of a network via gateway devices. Most of the solutions have developed cluster-based mesh routing protocols for improving nodes' connectivity and network stability [27]–[29]. However, in mobile mesh clients, the management of data delivery over the routing chains is one of the most important research problems. Moreover, wireless mesh provides their functionalities in an open architecture and malicious nodes can be served as mesh routers for data forwarding. In this case, various types of denial of service (DoS) attacks may be possible. As a result, the whole network communication could be interrupted and compromised [30]–[33].

This paper presents a robust and trusted routing scheme between mesh clients based on IoT devices to prevent network threats and achieves efficient data transmission systems. This paper aims to accomplish data reliability, confidentiality, authenticity with improved network throughput, energy efficiency, packets lost rate, computational overhead, and latency rate. The proposed secure and trusted scheme constructs robust routing channels among mesh devices and each mesh client forwards its data packets towards the default gateway using mesh routers. Moreover, the mesh clients are mobile to increase the network coverage with minimum overheads in data collection. The routing decision in the proposed scheme performs a crucial function in the delivery performance and reduces the probabilities incur in the transmission of duplicates data packets. In the proposed scheme, the avoidance of transmitting duplicate data packets and frequent route-rediscoveries between mesh clients significantly improves communication overheads and achieves a fault detection transmission system. Also, the proposed scheme incorporates a factor of link costs based on packets lost rate to achieve stable and error-free routing. The proposed scheme selects data transmission routes between mobile mesh clients and gateways based on the exploration of the communication channel. Accordingly, the transmission links are regularly re-structured by evaluating the link performance between mesh clients, which results in improving network connectivity and throughput in a timeous way. Moreover, in the proposed scheme, mesh clients are mobile and revolve in the observing field on periodic intervals thereby able to collect the monitoring data to attain high transmission rates with minimal delay and efficient energy utilization. Furthermore, mesh clients are operated in an open architecture and various security attacks can manipulate, disclose, or hide information from network users. Such network threats degrade the network security and give several opportunities to unauthorized nodes for data capturing and re-directing data packets towards prohibited routes. Therefore, the proposed scheme also develops an efficient and trusted hop by hop data routing pattern based on the RSA public-private key cryptography, which results in to increase the level of security against unreliable nodes. In the proposed scheme, network security is achieved by using the node's trustworthiness, integrity, and reliability. Our proposed security technique is also applicable for both fully and partially connected wireless mesh devices. The proposed security technique defends on the network data and information from external sources on the Internet. The article is organized in the subsequent subsets. Section 2 explains the background study and problem identification. Section 3 highlights the description of the proposed scheme against security threats with improved routing delivery ratios in the IoT-based mobile wireless mesh networks. The experimental results and discussion against related solutions are debated in Section 4. Section 5 concludes the article and highlights future work

II. BACKGROUND STUDY

The domain of wireless mesh networks is normally categorized with the number of mesh clients that are deployed randomly in the monitoring area. All mesh clients are connected in a multi-hop mode with wireless media in an ad-hoc manner. Mesh clients can join or leave any network infrastructure without affecting the rest of the communications [34], [35]. The foremost role of mesh clients is taking the information and forwarding it towards the destination via gateway points. The integration of several physical objects with mesh clients delivers a new class of application using IoT-based mesh networks [36]–[38]. Besides, due to the open architecture of wireless mesh networks integrated with IoT, data routing is more prone to DoS attacks. Such attacks may be harmful to network resources where information can be forwarded to unauthorized nodes. Also, DoS attacks are crucial for smart environmental applications and lead to a compromised network performance [39]–[42]. Moreover, due to DoS attacks, the information or resources can be unavailable to network users by temporarily disrupting the services of mesh clients. Consequently, to improve the routing performance in a mesh network concerning data privacy and network throughput, there is a need to construct a lightweight and secure data forwarding chains. In this way, only the information can be forwarded towards authorized mesh clients and leads to the trustworthiness of paths [43], [44]. Over the Internet, a lot of malicious nodes capturing and altering the data of devices without any permission. Therefore, data confidentiality, integrity, and authentications are major cryptographic goals and several researchers have proven that such goals must be integrated with the designing and developing process of any secure and trusted solution. The security challenges are growing over the Internet, thus, the proposed solution has to be ever-improving against network threats [45]–[48].

Authors in [49] have proposed a detection approach by using a zone-based hierarchical network model. To detect DoS attacks, end to end authentication, transmission rate, two-threshold value, and distributing voting parameters are used. The proposed approach improves network reliability and routing performance in the presence of DoS threats. Similarly, authors in [50] have described different network threats to present an effective secure key management scheme (SKeMS) for wireless mesh networks. In their proposed scheme, the encryption keys are secure forwarded between nodes and improves the results of network reliability and data security.

The proposed solution in [51] develops an efficient routing anomaly detection in wireless mesh networks. This solution aims to identify the selfish node among mesh clients. The proposed solution exploits the statistical theory of inference to achieve reliable clustering by using the node's local observations. The proposed solution is evaluated and compared with the existing work in terms of packet drop, detection, and fast alarm rates. The authors in [52] have proposed privacy preserved and secured reliable routing protocol for wireless mesh networks that aim to ensure confidentiality, reliability, and secure routing among mesh nodes. The proposed solution integrates the ID-based encryption, group signatures, and CLSL-DR mechanism to measure its performance with the relevant work. The experimental results demonstrate better outcomes as compared to other solutions in terms of different network parameters.

In [53], the authors have proposed a monitoring technique for wormhole-free routing and DoS attack defense in wireless mesh networks. In the beginning, all nodes keep track of their neighbors' receivers and senders' information based on the finite state model. Afterward, by using a wormhole-aware, a secure routing scheme is developed to identify the wormhole free paths over the network field. In the end, based on the priority mechanism, the data packets are forwarded towards end-points according to their priorities. The simulation results demonstrate that the proposed technique increases the packet delivery ratio and reduces the packet drop rate in the presence of DoS attacks. In [54], the authors proposed a security architecture to cope with the detection of network attacks and their authentication for wireless mesh networks. Based on the trusted routers, the proposed architecture offers security and identifies cloned AP and internal attacks. In the proposed architecture, the gateway devices are compared to the new arrived AP information with their stored databases to identify an attack. In [55], the authors have proposed the solution for optimizing the quality of service in the peer to peer wireless mesh networks. In this solution, the authors first examined the service quality and then offers an approach to improve service quality. The proposed solution makes use of the capability of profiting data transfer and utilizes the information to identify the overcrowd nodes in data routing. The authors in [11] proposed a load balance link layer protocol (LBLP), which aims to mutually handle the interfaces and communication medium for increasing the network throughput and balancing the traffic load in wireless mesh networks. The proposed solution also investigates how to reduce the network overhead in the presence of a large switching delay. In [56], the authors proposed a weighted trusted routing mechanism to identify and exclude the malicious nodes in the routing paths for wireless mesh networks. The proposed solution utilizes Dijkstra's routing algorithm for the calculation of the shortest routing path. However, the weighted value for edge is based on three different performance parameters i.e. node distance, trust value of node and packet lost. The proposed solution improves the network performance results in terms of network throughput, end-to-end delay and packet loss ratio.

Based on the related studies, it has been noticed that the majority of work has identified the significance of security for wireless mesh networks. The ultimate goal of providing security among mesh clients is to improve the data delivery ratio with a minimum delay rate. Besides, a few approaches have been designed to persist network scalability with efficient routing performance for mobile wireless mesh networks based on IoT. However, most of the proposed solutions suffer from reliable and timely data delivery due to the integration of mobile mesh clients. Furthermore, the majority of solutions adopt the routing paths by using only the hop-count factor and ignore the analysis of other parameters, which has great importance for data transmissions in an open architecture. Moreover, mobile mesh clients can leave or join the network deployment at any time, such mechanism may guide adversary nodes to be a part of the existing infrastructure thereby data packets can be dropped or may negotiate their integrity. Thus, a robust and trusted scheme must be designed to prevent security attacks in the presence of adversary nodes for IoT-based mobile wireless mesh networks, which results in improving the network stability and data privacy with an efficient delivery rate.

III. PROPOSED SCHEME

In this section, a summary of the proposed scheme is explained. The main aim of the proposed scheme is to design and develop the major techniques for achieving efficient, secured and robust routing in wireless mesh networks. The proposed scheme consists of two main functional techniques i.e. the first one is the network infrastructure of mobile mesh clients with gateways and the second one is secure and trusted data routing between mesh devices. In the first technique, all mesh clients, routers, and gateway devices are interconnected via a multi-hop model to construct an initial topological infrastructure as illustrated in Fig.1. Based on each constructed topological infrastructure, every mesh device constructs its routing table and creates an entry of the immediate neighbor node based on the least distance. Furthermore, based on the link estimation parameter, a reliable and efficient delivery path is determined between mesh clients, routers, and gateway devices for better-quality delivery performance. Unlike other most of the existing wireless mesh network solutions that deploy static network topology, the proposed scheme exploits mobile mesh clients to collect information from the environmental field and forward it towards the base station (BS), which is treated as the default gateway.

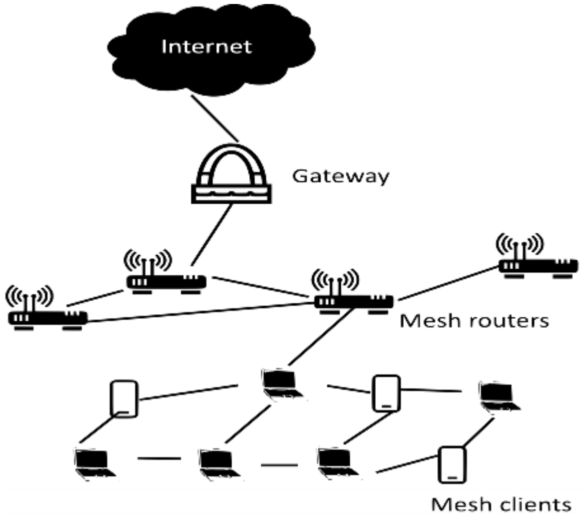

FIGURE 1. The architecture of wireless mesh networks.

Wireless mesh network provides various functionalities in open space and such an insecure environment provides a gap for adversary nodes to be part of the existing infrastructure, as a result, network security, authenticity, and data integrity may be compromised. The second technique of the proposed scheme is to secure data communications among mobile mesh devices with minimal computational overhead. The proposed mechanism greatly reflects the network performance in terms of dependability and packet drop ratio.

Fig.2 illustrates the proposed robust and trusted scheme for IoT-based mobile wireless mesh networks. Also, the proposed scheme is analyzed with other solutions in terms of network throughput, packets drop rate, latency rate, computational overheads, and energy efficiency factors. The experimental results demonstrate that the proposed scheme is trusted and robust, as it improves network throughput, energy efficiency with least packets drop ratio, network latency rate and computational overheads in the presence of malicious nodes.

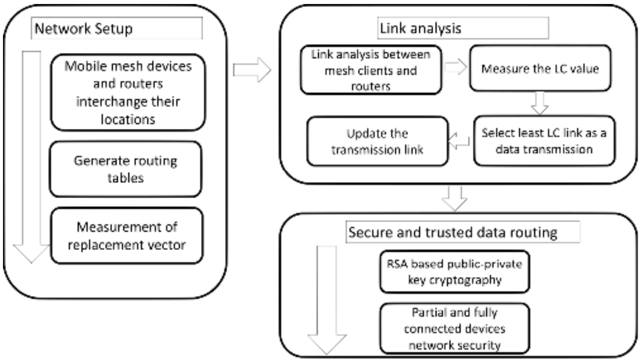
Network Setup
Mobile mesh devices and routers interchange their locations
Generate routing tables
Measurement of replacement vector
Link analysis
Link analysis between mesh clients and routers
Measure the LC value
Select least LC link as a data transmission
Update the transmission link
Secure and trusted data routing
RSA based public-private key cryptography
Partial and fully connected devices network security

FIGURE 2. Proposed robust and trusted scheme.

A. THE NETWORK INFRASTRUCTURE OF MOBILE MESH CLIENTS WITH GATEWAYS

In the first technique, all mesh clients including mesh routers flood their position data to construct the initial routing table. The routing table is updated each time when any new mesh client joins or existing one leaves the network infrastructure. At the start, each mesh node advertises a LOC message in the field that comprises two sub-fields. One is the node's unique ID and the other one is its current position. Upon receiving the data, each mesh client registers it in the routing table and further floods the data. However, a source mesh client may get several discovery messages from the neighbor mesh clients. In such a case, the priority is given to the least distance mesh clients and accordingly only the valid data is stored in the local routing table. The same practice is followed to collect the routing information from mesh clients to mesh routers. The constructed routing tables on each mesh device help to identify the appropriate neighbor node for data routing. After the formation of routing tables, all one-hop mesh clients towards the mesh router can transmit their data packets directly. While the mesh clients that are two or more hops away from the mesh router will make the use of a multi-hop communication paradigm.

In the proposed scheme, mesh clients are mobile to change their positions at each instance of time. Let say (x_i, y_i) be the initial position of the mobile mesh client and x_f, y_f be its final position, then the displacement $d(x, y)$ of the mobile mesh client at any time interval Δt can be computed using Euclidean function, as given in Equation 1.

$$d(x, y) = \sqrt{(x_f - x_i)^2 + (y_f - y_i)^2} \tag{1}$$

Accordingly, the calculated value of the displacement distance for mobile mesh clients at a time t_0 is flooded in the network region. Afterward, the one-hop mesh clients directly forward their data packets to the mesh router. And the mesh router further forwards it to the received data packets towards the BS.

Moreover, to maintain reliable data transmissions between mesh-clients-to-mesh-router and from mesh-router-to-BS, the proposed scheme estimates the link cost (LC) based on the packet lost rate (PLR) that indicates the value of the percentage concerning sending packets. Moreover, the computed LC value is also stored in the routing table of each source mesh device and determining the consistent and stable data forwarding path. Based on the up to date routing tables, the mesh device learns the robust and error-free routing towards the destination. To determine the packets lost rate, each mesh client sends a beacon message to its neighbors. After the receiving of beacon messages in particular time intervals, each mesh client determines the PLR between its neighbors. Let T_x is the number of packets at a unit time (t_0) that are transmitted from source mesh client i and R_x is the number of received packets per unit time on the receiver side, then the PLR between the source mesh client and the receiver can be computed based on Equation 2.

$$PLR = R_x(t_0)/T_x(t_0) \tag{2}$$

The computed LC as given in Equation 3 is in the range of [0, 1] and the PLR has a value in the same range.

$$LC = 1 - PLR \tag{3}$$

Accordingly, the source mesh client will select the appropriate next-hop for data routing with the least LC value. A similar method is also adopted in the proposed scheme to establish a reliable routing path between mesh routers and the BS. In the proposed scheme, the calculated LC, as given in Equation 3, allows achieving a robust delivery ratio with better network coverage using a mobile wireless mesh network. Algorithm 1 describes the formation of network set-up and reliable data routing paths among mesh clients, mesh routers, and gateways.

After the selection of next-hop, the source mesh client unicasts an RREQ message and in response, the next-hop replies back with an ACK message. The same practice is repeated until a reliable routing chain is generated between mobile mesh clients towards the gateway.

Algorithm 1 Network Set-Up of Mobile Mesh Clients With Gateways

```
Procedure network set-up
 mesh clients N and gateway devices flood their
 positions
 Using position algorithm, each device constructs
 routing table
 Mobile mesh client determines distance-vector $d(x, y)$
 on regular time interval Δt based on
 $d\,(x, y) = \sqrt{(x_f - x_i)^2 + (y_f - y_i)^2}$
 for each mesh client$_i$ ∈ [1. N]

    Evaluate the link cost $LC = 1 - PLR$ where $PLR =$
     $R_x(t_0)/T_x(t_0)$
     mobile_node$_i$ mesh client$_i$ selects the least LC link as a data
     transmission
     mesh client $i$ (update the routing table)
   end for
  for each mesh router$_i$ ∈ [1. MR]
     if(mesh router.next-hop = gateway BS$_{id}$)
       Data packets forwards directly
     end if
     while (destination! = gateway)
       evaluate LC and select the least computed value
       update the routing table accordingly
     end while
  end for
end procedure
```

B. SECURE AND TRUSTED DATA ROUTING BETWEEN MESH DEVICES

In this section, the proposed technique presents a fully secure and trusted data routing strategy. For secure data routing between the devices, an asymmetric-based RSA cryptographic technique is proposed which uses public-private keys [57], [58]. In the proposed technique, the mesh router generates key pairs (PU$_\mathrm{i}$, PR$_\mathrm{i}$) for each mesh client i using RSA based public key cryptography. In our proposed technique, the role of keys distribution (PU$_\mathrm{i}$, PR$_\mathrm{i}$) between mesh clients is performed by the mesh router. In this cryptographic technique, each mesh client possesses a pair of the public key (PU) and private key (PR), where the public key (PU) is distributed and is used to receive encrypted messages from the connecting neighboring mesh clients, and the private key (PR) (also known as the secret key) is used to decrypt the incoming messages towards the mesh client. The private key performs a vital role in data authentication and it must be kept secure from malicious and authorized nodes in the network.

In the proposed security technique, there are two topological scenarios: fully connected network topology and partially connected network topology. In a fully connected topological scenario, all the mesh clients are connected in a complete graph structure and use the public-private keys to encrypt and decrypt the data messages. If a node X wants to send a secure message ‘m’ to node Y, the message ‘m’ is encrypted to get ‘E(m)’ using the public key (PUY) of mesh client Y and then transmitted towards mesh client Y. On the reception of the encrypted message ‘E(m)’ from mesh client X, mesh client Y using its private key (PRY) decrypt the message. This communication is broadcasted towards all the mesh clients including the intended mesh client Y. In the meanwhile, those mesh clients with whom the message is not intended will ignore the message as they cannot decrypt the encrypted message without the appropriate private key.

In the case of partially connected topological scenario: If any mesh client X wants to send a message ‘m’ to mesh client Z, not directly connected to mesh client X. In the proposed technique, message ‘m’ from mesh client X will be encrypted ‘E(m)’ with the public key (PU_Z) of Z and broadcasted to all the connected mesh clients in the neighborhood of node X. Since the message is not intended to other mesh clients, they will re-broadcast the message to their neighbors in a multi-hop paradigm until it arrives at node Z. At the same time, each mesh client will send an acknowledgment ACK to the mesh client X for confirming the reception of the message.

This re-broadcasting process will eventually send the encrypted message to the intended mesh client Z, which will decrypt the message using its private key (PRZ) and at the same time, will send an acknowledgment message towards the sender. The sender will further transmit that acknowledgment towards the sending mesh client from which the message has arrived. This process continues until the message towards the intended mesh client Z is received from the sender node X. It must be noted that the proposed security technique not only preserves data security but also provides authentication by incorporating the public-private keys. The public-private keys in the proposed security technique make the robust authentication between mesh clients because if mesh client Z does not possess the matched private key, it will not be able to decrypt the incoming data messages. Algorithm 2 presents a secure and trusted data transmission based on RSA public-private cryptography.

Algorithm 2 Secure and Trusted Data Routing Based on RSA Public-Private Cryptography

```
Procedure secure and trusted transmission
    mesh clients attempt to forward data packets towards the
    gateway
    goto Algorithm 1 for the development of routing paths
    mesh routers share a pair of public-private key ($PU_i$, $PR_i$)
    between mesh clients
    data messsages are generated by mesh clients
    message ‘m’ from mesh client X encrypted as E(m) by
    ($PU_Z$)
      encrypted message ‘E(m)’ from mesh client X, mesh client
      Y using the private key
      (PRY) decrypt the message ‘m’
     intended mesh clients ignore the message ‘m’
      send an acknowledgment ACK to source mesh client X
      gateway devices verify the incoming messages
end procedure
```

IV. SIMULATION SETUP AND PARAMETERS

Table 1 illustrates the default network factors used in the experimental results and analysis. The proposed scheme is verified with security architecture for attack detection and authentication [54], and wormhole-free routing DoS attack defense [53] solutions. The experimental results of the proposed scheme with existing solutions are discussed based on a varying number of malicious and wireless mesh nodes. The variable speed of mesh clients is set in the range of 2 to 5 m/s. In the simulation environment of size (500, 500), the 50 to 250 mesh clients are deployed with 10 mobile mesh clients. The mesh routers are considered as a gateway device for data routing. The number of malicious nodes is fixed from 2 to 10. All the data traffic flows are based on a constant bit rate (CBR). The proposed scheme is evaluated in terms of network throughput, latency rate, packets lost rate, computational overhead, energy efficiency. All the experiments are done using a familiar network simulation (NS3) tool.

TABLE 1. Default network factors.

Factor	Value
Observing area	500m X 500m
Deployment	Random
Mesh clients	50 to 250
Malicious nodes	2 to 10
Packet size, k	250 bits
Key size	256 bits
Payload size	512 bytes
MAC layer	IEEE 802.11b
Control message	25 bits
Transmission range	25m
Simulation time	1000sec
Traffic flows	CBR

V. NUMERICAL RESULTS AND DISCUSSION

In this section, the experimental results of the proposed scheme are discussed in detail with respect to different network parameters.

A. ANALYSIS OF NETWORK THROUGHPUT

In this section, the simulation experiments are performed to evaluate the network throughput concerning a varying number of nodes in Fig.3. The experimental results demonstrate the improved performance of network throughput at an average of 16%. The proposed scheme augments the network throughput because of the selection of appropriate mesh clients for the forwarding data packets. Moreover, link estimation in the proposed scheme significantly improves the reliability between mesh clients and mesh routers. Furthermore, mobile mesh clients highly affect the delivery ratio of messages due to their periodic rotation for data gathering. Unlike other existing solutions, the proposed scheme monitors the updated position of mobile mesh clients and shifts the routing path on the network demand. As a result, the routing channels are kept more stable that leads to efficient network performance.

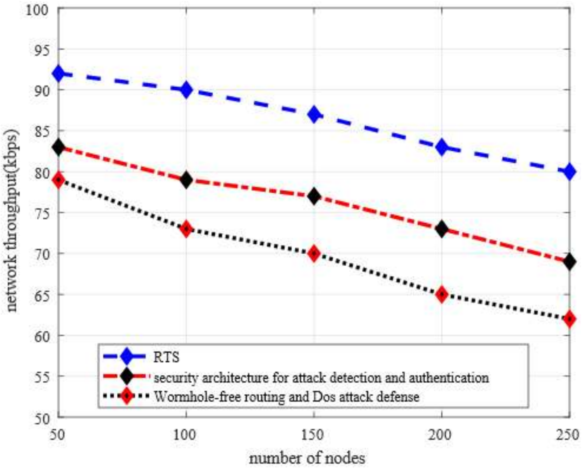

FIGURE 3. The impact of the number of nodes on network throughput.

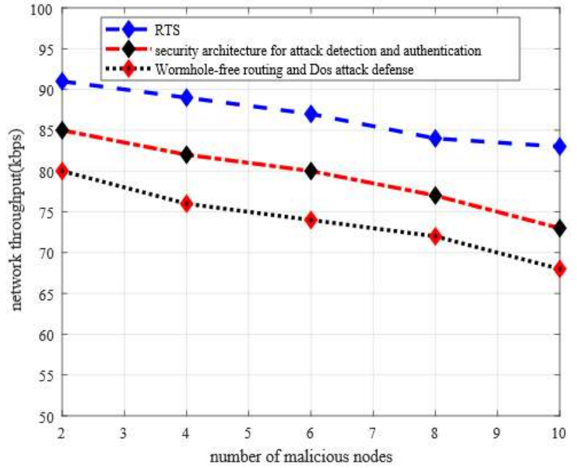

FIGURE 4. The impact of the number of malicious nodes on network throughput.

Fig.4 demonstrates the network throughput for a varying number of malicious nodes. The experimental results of our proposed scheme demonstrate that the performance of network throughput is increased by 12% as compared to existing solutions. Such improvement is due to authentic with reliable data security mechanisms based on public-key cryptography. The use of public-key cryptography in the proposed scheme is to achieve robust authentication and data confidentiality. In this case, a malicious node may not be able to capture, drop and change the contents of data packets. Also, most of the existing solutions do not consider the link estimation factor between the mesh clients and mesh router to achieve stable and trusted data routing. Such deficiency incurs an adverse influence on network throughput and efficacy of routing performance.

B. ANALYSIS OF PACKETS LOST RATE

Fig.5 illustrates the evaluation performance of the proposed scheme with existing solutions in connection to different numbers of nodes. The experimental results demonstrate that the proposed scheme has decreased the packets lost rate at an average of 37% in comparison with other solutions. Unlike other schemes that degrade the packets delivery ratio due to unstable and insecure data links, the proposed scheme decreases the packets lost rate due to the selection of the most reliable and secure mesh clients for data routing. Moreover, in a higher number of nodes, the proposed scheme generates the least congestion and equal balancing of load among mesh clients due to the incorporation of link estimation factors. The proposed scheme computes the packets lost rate factor for the link measurement between source and destination devices and achieves an improved message delivery ratio without sending extra control messages for the re-construction of routes. Furthermore, the proposed scheme offers security for network data based on public-key cryptography, which makes authentication and data encryption more secure and detects the anomalous actions under the presence of malicious nodes. Such a detection mechanism against malicious activities gives a significant impact on network performance and reduces the probability of manipulating, stolen and packets lost rate.

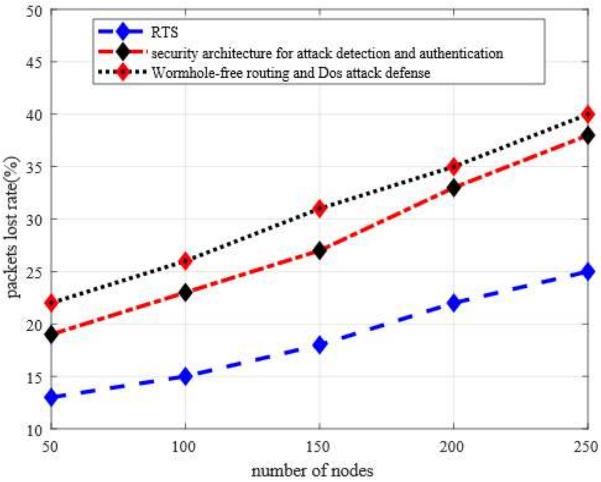

FIGURE 5. The impact of the number of nodes on the packet loss rate.

Fig.6 demonstrates the exploration of packets lost rate among the proposed scheme and the existing solutions. Under a varying number of malicious nodes, the proposed scheme reduces the packet loss rate by an average of 37% in comparison with other solutions. This is due to the selection of trustworthiness and stable routing paths between mesh clients and mesh gateway devices. Likewise, most of the existing solutions lack the mechanism for data integrity, as a result, malicious node may be a part of the source network that can lead to packets redirecting and dropping. In the proposed scheme, only legal nodes may take apart of forwarding the data packets towards the destination and all the engaged nodes in the routing paths are secured based on cryptography methods. Furthermore, most of the existing solutions make the use of static mesh clients and they do not cover all the monitoring area, therefore, a huge amount of data packets are

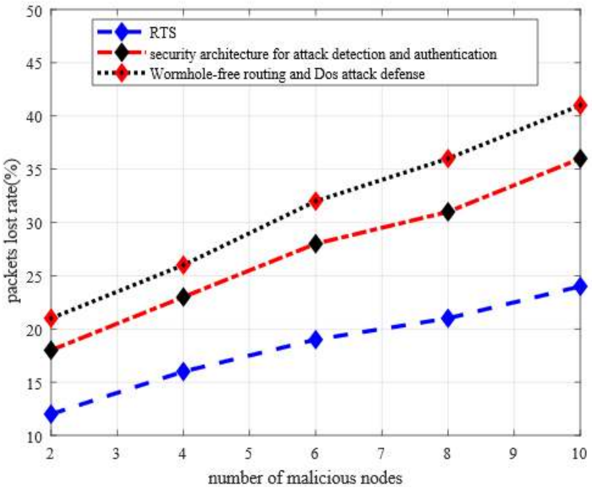

FIGURE 6. The impact of the number of malicious nodes on the packets lost rate.

unreachable towards the destination. In the proposed scheme, mobile mesh clients significantly improve network coverage and increase packets delivery ratio.

C. ANALYSIS OF LATENCY RATE

Fig.7 demonstrates the analysis of the latency rate among the proposed scheme and existing solutions. It is seen from the experimental results that the proposed scheme significantly decreases the latency rate in the average of 11.2%, as compared to other solutions. In higher network topologies, concerning the number of nodes, the proposed scheme chooses the most consistent and adaptive data forwarders between mesh client and gateway devices based on network parameters and environment conditions. Also, the condition of wireless channels is regularly re-determined for route stability and consistency. Such an adaptive routing mechanism provides better network delivery performance and reduces the probability of a higher latency ratio. Mobile mesh clients explicitly advertise their fresh positions based on the Euclidean distance method on a predefined time interval and lead to decrease chances for packets re-transmission with minimum delivery rates. Moreover, in a high network scenario under the different number of nodes, the proposed scheme produces less latency with the selection of minimal congested transmission paths due to the incorporation of the link estimation parameter.

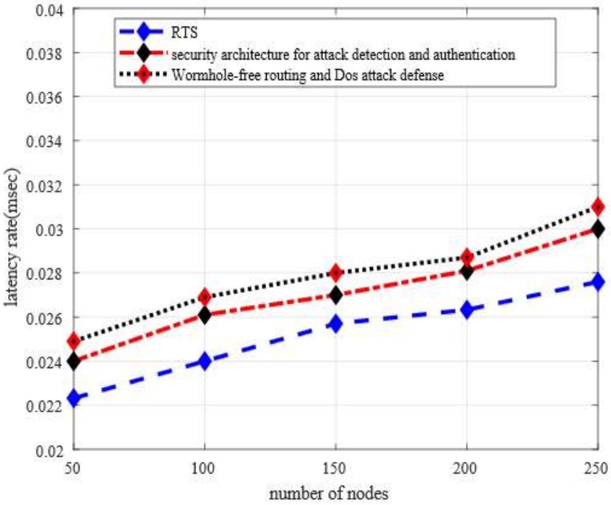

FIGURE 7. The impact of the number of nodes on the latency rate.

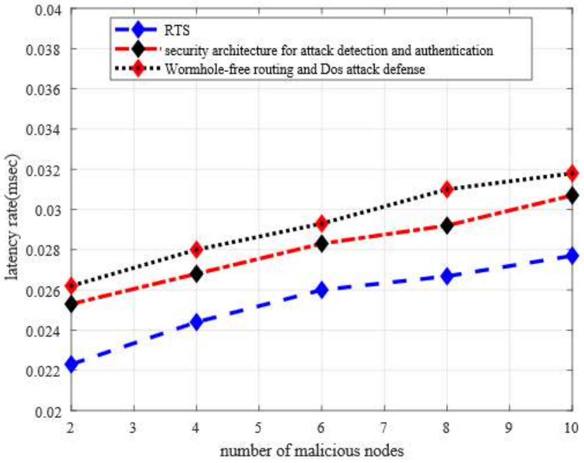

FIGURE 8. The impact of the number of malicious nodes on latency rate.

Fig.8 illustrates the latency rate of the proposed scheme is compared to the existing solutions in connection to a varying number of malicious nodes. Noticeably, it is seen that under a varying number of malicious nodes, the ratio of latency increases. However, the experimental results exhibit that the proposed scheme improves the latency rate at 13% in comparison with the existing solutions. The reason for such improvement is the construction of more efficient, robust, and secure routing channels among mesh clients and mesh routers. Moreover, the routing channels are updated based on the node's need. Also, mobile mesh clients significantly reduce the delivery delay while collecting the data packets from the monitoring field. Furthermore, the identification of wireless channels for data routing is rotated based on the analysis of link valuation. In the proposed scheme, the support of RSA public-private key cryptography reduces the possibilities of data re-transmissions and re-routing of data packets due to the development of a secure and realistic mechanism thereby reducing the network delay ratio.

D. ANALYSIS OF COMPUTATIONAL OVERHEAD

Fig.9 demonstrates the analysis of computational overhead between the proposed scheme and the existing solutions. It is seen from experimental results that the proposed scheme, as compared to the existing solutions, decreases the computational overhead by an average of 28%. The improvement in computational overhead is due to that the proposed scheme

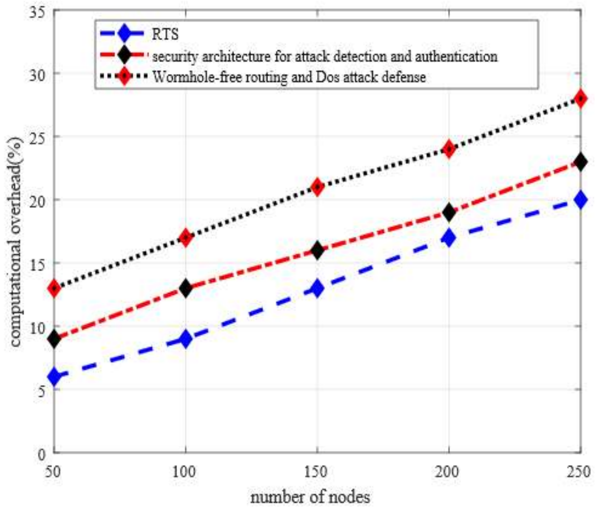

FIGURE 9. The impact of the number of nodes on computational overhead.

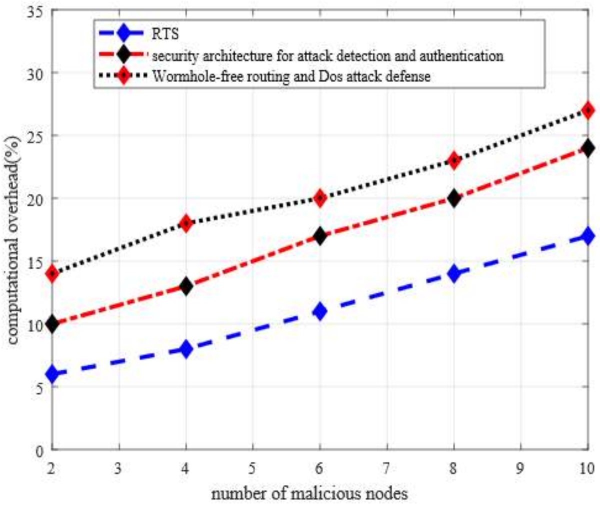

FIGURE 10. The impact of the number of malicious nodes on computational overheads.

decreases the chances of malicious attacks by introducing the data reliability and efficient routing. The proposed data security technique offers data protection against route breakages and avoids the chances of data retransmissions, which results in an improvement in the network overhead. Moreover, based on the Euclidean distance, the proposed scheme measures the up-to-date displacement vector of mobile mesh clients and improves network coverage and decreases the extra burden of control messages between mesh devices. Unlike other solutions, the proposed scheme makes the use of mobile mesh clients, determines their latest position on the specific time interval and decreases the communication overheads while data aggregation and forwarding. Also, unlike prefixed and static data forwarders, the proposed scheme decreases the unnecessary computation overheads by measuring the links status and network conditions for the formation of optimal routes among mesh clients and mesh gateways.

Fig.10 illustrates the computational overhead of the proposed scheme and existing solutions under a varying number of malicious nodes. The simulation results reveal that the proposed scheme in comparison with the existing solutions significantly decreases computational overhead by an average of 40%. The existing solutions suffer unnecessary computational overhead in data re-routing and re-formation of routing paths in the existence of the adversary environment. The proposed scheme offers an authentic and secure public-key cryptography mechanism, which gives network privacy and data integrity. Also, it greatly reduces the packets drop ratio and ultimately requires less computational overhead for data routing in the presence of malicious nodes. Moreover, the mesh router securely generates and distributes the private-public keys based on the RSA algorithm and ultimately mesh clients need no additional computational power to achieve data security. Due to more secure and authentic routing channels, the proposed scheme reduces the probabilities of re-routing of data packets towards authorized nodes and such mechanism ultimately decreases the computation overhead on nodes level. Further, the existing solutions present extra computational overheads particularly in a scalable network size because of the inefficient identification of malicious nodes.

E. ANALYSIS OF ENERGY EFFICIENCY

Fig.11 illustrates the performance of the energy efficiency of the proposed scheme with existing solutions. The simulation experiments have shown that the proposed solution improved the energy efficacy by 21% as compared to other solutions. This is to the selection of optimal routing paths for data transmission between mesh clients and mesh gateways. Also, the proposed scheme imposes low computational overheads on nodes level which leads to balance the battery consumption of mesh clients. The proposed balanced energy

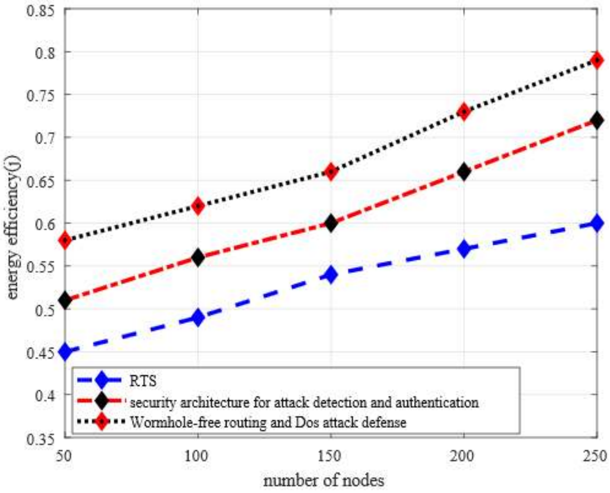

FIGURE 11. The impact of the number of nodes on energy efficiency.

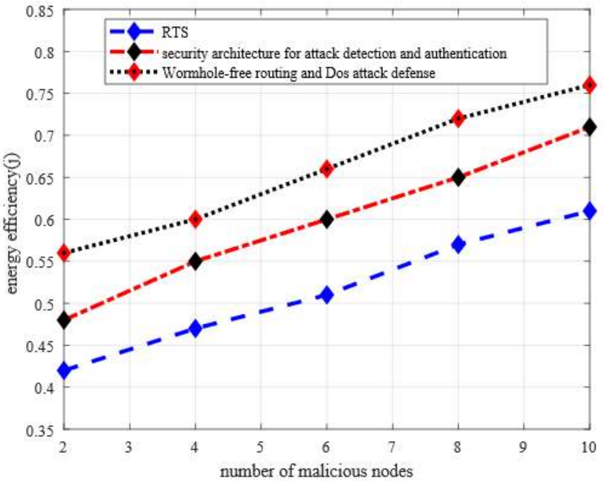

FIGURE 12. The impact of the number of malicious nodes on energy efficiency.

consumption in the network field because of the use of mobile mesh clients and shortened the routes for data transmissions. Besides, under a varying number of mesh clients, the proposed scheme securely identifies the malicious nodes and a result, unnecessary data traffic caused by malicious nodes is prevented thereby eliminating irrelevant data forwarding by mesh clients and improved energy efficiency of the network.

Fig.12 demonstrates the analysis of the energy efficiency of the proposed scheme in the comparison of existing solutions. The experimental results have proven in the presence of malicious nodes, our proposed scheme significantly offers efficient energy consumption by 18% as compared to the existing solutions. This reason for this improvement is that the proposed scheme maintains a local information table on nodes level and only updates the table whenever any change incurred in the neighbors. Moreover, the evaluation of the link factor in the transmission system, the proposed scheme significantly decreases the chances of data re-sending which ultimately increases the energy efficiency of the network. Furthermore, the mesh routers are appointed as a central organizer to generate and distribute the keys among mesh clients, which results in decreasing additional energy consumption on the part of mesh clients. Moreover, the generation of optimal routes between mesh clients to gateways and from gateways to end users, the proposed scheme increasing the lifetime of routes, which results in efficient utilization of battery power of the mesh clients.

VI. CONCLUSION

This paper presents a robust and trusted scheme for IoT-based mobile wireless mesh networks, which aim to improve the coverage and reliability of the network infrastructure. Also, transmission links between mesh clients and gateways are secured under the presence of malicious nodes based on the RSA public-private cryptography. In the majority of the existing works, they proposed data routing schemes for static mesh nodes and overlooked the link estimation. Such a solution incurs a negative impact on network performance and raises the probability of packets drop ratio. The proposed scheme comprises mobile mesh clients for better network exposure and evaluates the transmission links based on the packets drop rate factor, thus, the proposed scheme achieves improved data delivery ratios. Furthermore, mobile mesh clients flood their distance vector on periodic intervals and overcome communication costs. The simulation results demonstrate that the proposed scheme increases the data reliability and with minimal computational overheads in varying network topologies. However, the proposed scheme incurs additional network costs in generating and distributing the pairs of public-private keys between mesh devices. In future work, the proposed scheme will be further enhanced to tackle other DOS threats i.e. non-repudiation and replay, which crack network set-ups and functionalities. Also, the proposed scheme may include some machine learning-based optimization techniques to make the mesh clients intelligent with nominal node level and processing overhead.

REFERENCES

[1] K. M. Modieginyane, B. B. Letswamotse, R. Malekian, and A. M. Abu-Mahfouz, "Software defined wireless sensor networks application opportunities for efficient network management: A survey," *Comput. Electr. Eng.*, vol. 66, pp. 274–287, Feb. 2018.

[2] L. Kumar, V. Sharma, and A. Singh, "Feasibility and modelling for convergence of optical-wireless network–a review," *AEU-Int. J. Electron. Commun.*, vol. 80, pp. 144–156, Oct. 2017.

[3] K. Haseeb, N. Islam, A. Almogren, and I. U. Din, "Intrusion prevention framework for secure routing in WSN-based mobile Internet of Things," *IEEE Access*, vol. 7, pp. 185496–185505, 2019.

[4] K. A. Awan, I. U. Din, A. Almogren, M. Guizani, and S. Khan, "StabTrust—A stable and centralized trust-based clustering mechanism for IoT enabled vehicular ad-hoc networks," *IEEE Access*, vol. 8, pp. 21159–21177, 2020.

[5] E. Luo, Q. Liu, J. H. Abawajy, and G. Wang, "Privacy-preserving multihop profile-matching protocol for proximity mobile social networks," *Future Gener. Comput. Syst.*, vol. 68, pp. 222–233, Mar. 2017.

[6] S. Barrachina-Muñoz, B. Bellalta, T. Adame, and A. Bel, "Multi-hop communication in the uplink for LPWANs," *Comput. Netw.*, vol. 123, pp. 153–168, Aug. 2017.

[7] D. Jiang, W. Li, and H. Lv, "An energy-efficient cooperative multicast routing in multi-hop wireless networks for smart medical applications," *Neurocomputing*, vol. 220, pp. 160–169, Jan. 2017.

[8] J. Li, B. N. Silva, M. Diyan, Z. Cao, and K. Han, "A clustering based routing algorithm in IoT aware wireless mesh networks," *Sustain. Cities Soc.*, vol. 40, pp. 657–666, Jul. 2018.

[9] Y. Chai, W. Shi, and T. Shi, "Load-aware cooperative hybrid routing protocol in hybrid wireless mesh networks," *AEU-Int. J. Electron. Commun.*, vol. 74, pp. 135–144, Apr. 2017.

[10] M. Boushaba, A. Hafid, and M. Gendreau, "Node stability-based routing in wireless mesh networks," *J. Netw. Comput. Appl.*, vol. 93, pp. 1–12, Sep. 2017.

[11] X. Deng, J. Luo, L. He, Q. Liu, X. Li, and L. Cai, "Cooperative channel allocation and scheduling in multi-interface wireless mesh networks," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 1, pp. 1–12, Jan. 2019.

[12] C.-C. Lin, P.-T. Tseng, T.-Y. Wu, and D.-J. Deng, "Social-aware dynamic router node placement in wireless mesh networks," *Wireless Netw.*, vol. 22, no. 4, pp. 1235–1250, May 2016.

[13] A. K. Kiani, R. F. Ali, and U. Rashid, "Energy-load aware routing metric for hybrid wireless mesh networks," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, May 2015, pp. 1–5.

[14] H. A. Khattak, Z. Ameer, U. I. Din, and M. K. Khan, "Cross-layer design and optimization techniques in wireless multimedia sensor networks for smart cities," *Comput. Sci. Inf. Syst.*, vol. 16, no. 1, pp. 1–17, 2019.

[15] P. Fraga-Lamas, L. Ramos, V. Mondéjar-Guerra, and T. M. Fernández-Caramés, "A review on IoT deep learning UAV systems for autonomous obstacle detection and collision avoidance," *Remote Sens.*, vol. 11, no. 18, p. 2144, 2019.

[16] F. Castaño, S. Strzelczak, A. Villalonga, R. E. Haber, and J. Kossakowska, "Sensor reliability in cyber-physical systems using Internet-of-Things data: A review and case study," *Remote Sens.*, vol. 11, no. 19, p. 2252, 2019.

[17] K. A. Awan, I. U. Din, A. Almogren, M. Guizani, A. Altameem, and S. U. Jadoon, "Robusttrust–a pro-privacy robust distributed trust management mechanism for Internet of Things," *IEEE Access*, vol. 7, pp. 62095–62106, 2019.

[18] H.-C. Lee and K.-H. Ke, "Monitoring of large-area IoT sensors using a LoRa wireless mesh network system: Design and evaluation," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 9, pp. 2177–2187, Sep. 2018.

[19] E. Di Pascale, I. Macaluso, A. Nag, M. Kelly, and L. Doyle, "The network as a computer: A framework for distributed computing over IoT mesh networks," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2107–2119, Jun. 2018.

[20] K. Haseeb, N. Islam, A. Almogren, I. U. Din, H. N. Almajed, and N. Guizani, "Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs," *IEEE Access*, vol. 7, pp. 79980–79988, 2019.

[21] K. A. Awan, I. U. Din, M. Zareei, M. Talha, M. Guizani, and S. U. Jadoon, "Holitrust-a holistic cross-domain trust management mechanism for service-centric Internet of Things," *IEEE Access*, vol. 7, pp. 52191–52201, 2019.

[22] I. U. Din, M. Guizani, S. Hassan, B.-S. Kim, M. K. Khan, M. Atiquzzaman, and S. H. Ahmed, "The Internet of Things: A review of enabled technologies and future challenges," *IEEE Access*, vol. 7, pp. 7606–7640, 2019.

[23] I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the Internet of Things: A survey," *IEEE Access*, vol. 7, pp. 29763–29787, 2019.

[24] W. G. Diancin, "Intelligent sequencing of multiple wireless nodes for transfer between wireless mesh networks in a process control system," U.S. Patent 10 334 458, Jun. 25, 2019.

[25] S. Kafaie, Y. Chen, O. A. Dobre, and M. H. Ahmed, "Joint inter-flow network coding and opportunistic routing in multi-hop wireless mesh networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 2, pp. 1014–1035, 2nd Quart., 2018.

[26] U. Ullah, A. Khan, M. Zareei, I. Ali, H. A. Khattak, and I. U. Din, "Energy-effective cooperative and reliable delivery routing protocols for underwater wireless sensor networks," *Energies*, vol. 12, no. 13, p. 2630, 2019.

[27] S. Liu, K. Liu, J. Zhang, T. Zhang, Z. Xu, and F. Liu, "A location and cluster-based MAC and routing protocol for wireless mesh networks," in *Proc. 2nd IEEE Adv. Inf. Manage., Communicates, Electron. Autom. Control Conf. (IMCEC)*, May 2018, pp. 1963–1969.

[28] Y. M. Rao, M. V. Subramanyam, and K. S. Prasad, "Cluster based hybrid routing protocol for wireless mesh networks," *Wireless Pers. Commun.*, vol. 103, no. 4, pp. 3009–3023, Dec. 2018.

[29] A. Bozorgchenani, M. Jahanshahi, and D. Tarchi, "Gateway selection and clustering in multi-interface wireless mesh networks considering network reliability and traffic," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 3, p. e3215, Mar. 2018.

[30] S. K. Gupta, "Wireless Mesh Network Security, Architecture, and Protocols," in *Security and Privacy Issues in Sensor Networks and IoT*. Hershey, PA, USA: IGI Global, 2020, pp. 1–27.

[31] A. Nanda, P. Nanda, X. He, A. Jamdagni, and D. Puthal, "A hybrid encryption technique for Secure-GLOR: The adaptive secure routing protocol for dynamic wireless mesh networks," *Future Gener. Comput. Syst.*, early access, Jun. 6, 2018, doi: 10.1016/j.future.2018.05.065.

[32] A. Sgora and D. D. Vergados, and P. Chatzimisios, "A survey on security and privacy issues in wireless mesh networks," *Secur. Commun. Netw.*, vol. 9, no. 13, pp. 1877–1889, 2016.

[33] K. Haseeb, A. Almogren, N. Islam, I. U. Din, and Z. Jan, "An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN," *Energies*, vol. 12, no. 21, p. 4174, 2019.

[34] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," *Comput. Netw.*, vol. 47, no. 4, pp. 445–487, Mar. 2005.

[35] A. B. M. A. Al Islam, M. J. Islam, N. Nurain, and V. Raghunathan, "Channel assignment techniques for multi-radio wireless mesh networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 2, pp. 988–1017, 2nd Quart., 2016.

[36] D. Mars, S. M. Gammar, A. Lahmadi, and L. A. Saidane, "Using information centric networking in Internet of Things: A survey," *Wireless Pers. Commun.*, vol. 105, no. 1, pp. 87–103, Mar. 2019.

[37] M. Bembe, A. Abu-Mahfouz, M. Masonta, and T. Ngqondi, "A survey on low-power wide area networks for IoT applications," *Telecommun. Syst.*, vol. 71, no. 2, pp. 249–274, Jun. 2019.

[38] L. Leonardi, G. Patti, and L. L. Bello, "Multi-hop real-time communications over Bluetooth low energy industrial wireless mesh networks," *IEEE Access*, vol. 6, pp. 26505–26519, 2018.

[39] J. Sen, "Security and privacy issues in wireless mesh networks: A survey," in *Wireless Networks and Security*. Berlin, Germany: Springer, 2013, pp. 189–272.

[40] P. H. Pathak and R. Dutta, "A survey of network design problems and joint design approaches in wireless mesh networks," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 3, pp. 396–428, 3rd Quart., 2011.

[41] A. K. Roy and A. K. Khan, "Architectural and security prospective of wireless mesh network," *Int. J. Comput. Intell. IoT*, vol. 2, no. 1, pp. 1–5, 2019.

[42] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, "Intrusion detection systems for IoT-based smart environments: A survey," *J. Cloud Comput.*, vol. 7, no. 1, p. 21, Dec. 2018.

[43] L. Zhang, X. Wang, Y. Jiang, M. Yang, T. Mak, and A. K. Singh, "Effectiveness of HT-assisted sinkhole and blackhole denial of service attacks targeting mesh networks-on-chip," *J. Syst. Archit.*, vol. 89, pp. 84–94, Sep. 2018.

[44] E. A. Shams and A. Rizaner, "A novel support vector machine based intrusion detection system for mobile ad hoc networks," *Wireless Netw.*, vol. 24, no. 5, pp. 1821–1829, Jul. 2018.

[45] A. Al-Haj, G. Abandah, and N. Hussein, "Crypto-based algorithms for secured medical image transmission," *IET Inf. Secur.*, vol. 9, no. 6, pp. 365–373, Nov. 2015.

[46] L. O. M. Kobayashi, S. S. Furuie, and P. S. L. M. Barreto, "Providing integrity and authenticity in DICOM images: A novel approach," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 4, pp. 582–589, Jul. 2009.

[47] A. Bakshi and A. K. Patel, "Secure telemedicine using RONI halftoned visual cryptography without pixel expansion," *J. Inf. Secur. Appl.*, vol. 46, pp. 281–295, Jun. 2019.

[48] V. Adat and B. B. Gupta, "Security in Internet of Things: Issues, challenges, taxonomy, and architecture," *Telecommun. Syst.*, vol. 67, no. 3, pp. 423–441, Mar. 2018.

[49] L. Luan, Y. Fu, and P. Xiao, "An effective denial of service attack detection method in wireless mesh networks," *Phys. Procedia*, vol. 33, pp. 354–360, Jun. 2012.

[50] F. Kandah, Y. Singh, and W. Zhang, "Mitigating eavesdropping attack using secure key management scheme in wireless mesh networks," *J. Commun.*, vol. 7, no. 8, pp. 596–605, 2012.

[51] J. Sen, "Efficient routing anomaly detection in wireless mesh networks," in *Proc. 1st Int. Conf. Integr. Intell. Comput.*, Aug. 2010, pp. 302–307.

[52] N. T. Meganathan and Y. Palanichamy, "Privacy preserved and secured reliable routing protocol for wireless mesh networks," *Sci. World J.*, vol. 2015, pp. 1–12, Sep. 2015.

[53] G. Akilarasu and S. M. Shalinie, "Wormhole-free routing and DoS attack defense in wireless mesh networks," *Wireless Netw.*, vol. 23, no. 6, pp. 1709–1718, Aug. 2017.

[54] P. K. Sharma, R. Mahajan, and Surender, "A security architecture for attacks detection and authentication in wireless mesh networks," *Cluster Comput.*, vol. 20, no. 3, pp. 2323–2332, Sep. 2017.

[55] M. Gheisari, J. Alzubi, X. Zhang, U. Kose, and J. A. M. Saucedo, "A new algorithm for optimization of quality of service in peer to peer wireless mesh networks," *Wireless Netw.*, pp. 1–9, Mar. 2019.

[56] G. Rathee, H. Saini, and G. Singh, "Aspects of trusted routing communication in smart networks," *Wireless Pers. Commun.*, vol. 98, no. 2, pp. 2367–2387, Jan. 2018.

[57] P. Barrett, "Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1986.

[58] S. Srivastava and A. Srivastava, "Integration of RSA and waterfall framework: Aggrandize security in cloud computing using integration of Rivest–Shamir–Adleman (encryption algorithm) and waterfall model," *J. Microcontroller Eng. Appl.*, vol. 4, no. 3, pp. 1–8, 2018.

KHALID HASEEB received the MS-IT degree from the Institute of Management Sciences, Peshawar, Pakistan, and the Ph.D. degree in computer science from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia, in 2016. He has an experience of several years in teaching and research and development. He is currently an Assistant Professor with the Department of Computer Science, Islamia College Peshawar. His research interests include wireless sensor networks, ad-hoc networks, network security, the Internet of Things, software define networks, and sensors-cloud. He involves as a Referee for many reputed international journals and conferences.

IKRAM UD DIN (Senior Member, IEEE) received the M.Sc. degree in computer science and the M.S. degree in computer networking from the Department of Computer Science, University of Peshawar, Pakistan, and the Ph.D. degree in computer science from the School of Computing, Universiti Utara Malaysia (UUM). He was the IEEE UUM Student Branch Professional Chair. He has 12 years of teaching and research experience with different universities/organizations. He is currently a Lecturer with the Department of Information Technology, The University of Haripur. His current research interests include resource management, traffic control in wired and wireless networks, vehicular communications, mobility and cache management in information-centric networking, and the Internet of Things.

AHMAD ALMOGREN (Senior Member, IEEE) received the Ph.D. degree in computer science from Southern Methodist University, Dallas, Tx, USA, in 2002. He was the Vice Dean of the Development and Quality, College of Computer and Information Sciences (CCIS), King Saud University (KSU), Riyadh, Saudi Arabia. He was also the Dean of the College of Computer and Information Sciences and the Head of the Academic Accreditation Council with Al-Yamamah University. He is currently a Professor and the Director of the Cyber Security Chair with the Computer Science Department, CCIS, KSU. His research interests include mobile-pervasive computing and cyber security. He served as the General Chair for the IEEE Smart World Symposium and a Technical Program Committee Member in numerous international conferences/workshops, such as the IEEE CCNC, ACM, BodyNets, and the IEEE HPCC.

NAVEED ISLAM received the Ph.D. degree in computer science from the University of Montpellier II, France, in 2011. He is currently an Assistant Professor with the Department of Computer Science, Islamia College Peshawar, Pakistan. He is the author of numerous international journal articles and conference papers. His research interests include computer vision, information security, machine learning, artificial intelligence, and wireless sensor networks. He is a regular Reviewer of the IEEE, Elsevier, and Springer Journals.

AYMAN ALTAMEEM received the Ph.D. degree in information technology from the University of Bradford, U.K., and the M.Sc. degree in information systems from London South Bank University, U.K. He is currently the Dean of the College of Applied Studies and Community Services, King Saud University, Riyadh. His research interests include e-commerce, the Internet of Things, information security, and artificial intelligence.