technologies

Article

PDSCM: Packet Delivery Assured Secure Channel Selection for Multicast Routing in Wireless Mesh Networks

Seetha S [1], Esther Daniel [2], S Durga [3], Jennifer Eunice R [4,*] and Andrew J [5,*]

[1] Department of Information Science and Engineering, CMR Institute of Technology, Bengaluru 560037, Karnataka, India; sitamismin19@gmail.com
[2] Department of Computer Science and Engineering, Karunya Institute of Technology & Sciences, Coimbatore 641114, Tamilnadu, India; estherdaniel@karunya.edu
[3] Department of Information Technology, Sri Krishna College of Engineering & Technology, Coimbatore 641008, Tamilnadu, India; durgas@skcet.ac.in
[4] Department of Mechatronics Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, Karnataka, India
[5] Department of Computer Science and Engineering, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal 576104, Karnataka, India
* Correspondence: jennifer.r@manipal.edu (J.E.R.); andrew.j@manipal.edu (A.J.)

Abstract: The academic and research communities are showing significant interest in the modern and highly promising technology of wireless mesh networks (WMNs) due to their low-cost deployment, self-configuration, self-organization, robustness, scalability, and reliable service coverage. Multicasting is a broadcast technique in which the communication is started by an individual user and is shared by one or multiple groups of destinations concurrently as one-to-many allotments. The multicasting protocols are focused on building accurate paths with proper channel optimization techniques. The forwarder nodes of the multicast protocol may behave with certain malicious characteristics, such as dropping packets, and delayed transmissions that cause heavy packet loss in the network. This leads to a reduced packet delivery ratio and throughput of the network. Hence, the forwarder node validation is critical for building a secure network. This research paper presents a secure forwarder selection between a sender and the batch of receivers by utilizing the node's communication behavior. The parameters of the malicious nodes are analyzed using orthogonal projection and statistical methods to distinguish malicious node behaviors from normal node behaviors based on node actions. The protocol then validates the malicious behaviors and subsequently eliminates them from the forwarder selection process using secure path finding strategies, which lead to dynamic and scalable multicast mesh networks for communication.

Keywords: wireless mesh networks; multicasting; forwarder node validation; vindictive nodes

Citation: S, S.; Daniel, E.; Durga, S.; Eunice R, J.; J, A. PDSCM: Packet Delivery Assured Secure Channel Selection for Multicast Routing in Wireless Mesh Networks. *Technologies* **2023**, *11*, 130. https://doi.org/10.3390/technologies11050130

Academic Editor: Sotirios K. Goudos

Received: 31 July 2023
Revised: 1 September 2023
Accepted: 3 September 2023
Published: 18 September 2023

1. Introduction

Mobile communications' fifth generation (5G) is bringing about a variety of advancements for both business and end consumers. Because 5G communications operate at a relatively high frequency compared to earlier technologies, this new network faces a challenge that may limit its industrial application. One such challenge is that coverage is less extensive [1]. The coverage area is not as wide as intended when using such high frequencies. The best way to expand 5G services is to keep network infrastructure's capital costs to a minimum while also expanding 5G wireless communication coverage. By employing 5G network resources to build a wireless mesh network, it is possible to extend the reach of a 5G network across longer distances. There are many benefits to employing a wireless mesh network as a backhaul network in 5G networks, including a significantly lower setup cost. This is true since all wireless mesh networks require routers. The compatibility of the devices is the most crucial factor to consider when selecting a wireless mesh network. A greater number of end users can connect to the 5G network as a result of this.

Researchers have recently begun to look towards the following generation, known as the 6G network, even though the fifth-generation mobile network is currently being commercialized across the globe [2]. Sixth-generation ecosystems, in contrast to 5G, are seen as a platform for advancements in computing, artificial intelligence, connection and sensors, virtualization, and other fields. Whether it is part of a 5G or 6G mobile communication network, the wireless mesh network is a wonderful option to consider as a backhaul network for larger coverage, less infrastructure cost, and compatibility of the devices.

The adoption of wireless mesh networks (WMNs) has accelerated during the past 20 years in both industrialized and developing nations. WMNs are crucial in providing access to the internet [3]. The use of multicast communication technology is common in wireless situations with a lot of devices [4]. Many interesting applications such as news/sports/stock/weather updates, distance learning, content distribution, web-cache updates, etc., use the services of multicast routing protocols [5–8] as an effective way of sending a datagram to multiple receivers with single transmit operation.

Most of the existing multicast routing protocols [9–11] are focused on improving the quality-of-service requirements to achieve high throughput, minimize delay, minimize congestion, minimize the cost, etc. On the other hand, addressing security issues in a multicast environment is also important. Nodes in the multicast mesh networks must work together to compute the route metric and forward data. The confidence that all nodes are honest and perform accurately during metric computation and data transmission results in unsuspected outcomes where compromised nodes act maliciously by dropping packets, delaying transmissions that cause heavy packet loss in the network. This leads to a reduced packet delivery ratio and throughput of the network. Hence, the forwarder node validation is applied in PDSCM to build a secure network.

In PDSCM, the network validates the node behavior through sending and receiving the packet status of each node. The initial network node's behavior and the consecutive actions are computed by the number of iterations during the transmissions. This validates the malicious node behavior through the final orthogonal computational output and subsequently, the malicious node is removed from the network. The proposed protocol is focused on validating the forwarder node behavior using the two mathematical approaches; viz., the orthogonal projection method and statistical method. An orthogonal projection [12,13] is a set of matrix operations that describe the conditions of the independent behavioral changes of the nodes. The statistical method [14,15] constructs the lower and upper bound estimates for the honest node's (normal node) packet delivery ratio periodically.

The major contributions of this work are as follows:

1. Creation of data forwarding attacks in wireless mesh networks;
2. Computation of network metrics including ongoing delivery ratio and predictable delivery ratio;
3. Construction of route discovery phase using the PDSCM protocol;
4. Implementation of secure multicast routing using twin- and quad-based computing and the orthogonal projection algorithm;
5. Detection of data forwarding attacks and alternate path-finding mechanism.

The rest of the article is formulated as follows. Section 2 summarizes the security issues in multicast mesh networks based on previous investigations. Section 3 describes two important network metrics used in the proposed protocol. Section 4 explains the overview of the data forwarding attack. The objectives and steps carried out to find the multicast route in PDSCM without vindictive nodes are discussed in Section 5. In Section 6, results and discussions are analyzed along with those of the previous studies and shows the analysis of the time complexity of the proposed technique. The article concludes with Section 7.

2. Literature Survey

In this section, we briefly describe the existing secure multicast routing protocols in wireless mesh networks. The secure multicast routing protocols depend on the commu-

nication behavior of multicast routers to identify and avoid malicious nodes during path establishment. There are only a few secure multicast protocols found in the literature [16].

Multicast secure routing protocols such as hierarchical agent-based secure multicast (HASM) [17] focus on addressing the secure mobile multicast by guaranteeing multicast information access to genuine users. This approach reduces the total network communication cost but does not consider attacks that arise within the multicast group. The adaptive and bandwidth-reducing (ABR) tree [18] ensures data confidentiality in group communication and reduces bandwidth consumption associated with rekeying functionalities. The limitation of this approach is that the deletion event is not enhanced to a minimum cost level. Mesh certification authority (MeCA) [19] uses multicasting based on the Ruiz tree, which minimizes the operational cost associated with multicasting. MeCA has various features to verify, update, and securely revoke certificates of mesh nodes. This method suffers an additional overhead in moving MeCA functionalities. In the case of secure group overlay multicast (SeGrOM) [20], only authorized group members can send data to the group. The advantage of SeGrOM is that it earns minimum computational and communication overhead, at the same time ensuring security, but does not consider the attacks towards the multicast protocol itself.

Nevertheless, the secure on-demand multicast routing protocol (S-ODMRP) [21] is focused on selecting a path based on a high-quality metric to improve the throughput of the network with the intent to detect metric manipulation attacks. In such an approach, some normal nodes are falsely blamed based on the value of the threshold parameter. In the case of the secure multicast routing algorithm for wireless mesh network (SEMRAW) [22], the security framework is designed to guard against all active attacks in multicast routing. It employs digital signatures to prevent a malicious node from gaining unauthorized access to the multicast data. The limitation of this approach is that the routing overhead associated with SEMRAW is high, as it requires three additional addresses to find the attacker, and the computational complexity is also high, as it needs two signatures per packet of the multicast transmission.

Sharma, Bhawna, and Rohit Vaid [23] proposed a tree and mesh-based routing protocol using traffic encryption keys (TEKs) and private and public key infrastructure inside the multicast group to address the problem of key distribution. However, this protocol incurs additional overheads for key distribution and the maintenance of public and private keys.

Secure key management on ODMRP [24] for cellular ad hoc networks provides a mesh-based multicast key control mechanism in ODMRP that also ensures services such as excessive safety and availability, but this key control is achieved with additional overhead; viz., normalized routing load, average end-to-end latency, and control overhead average packet delay.

Network coding is a transmission paradigm that is used for optimizing the usage of network resources. According to network coding, every neighbor node before transmitting the data splits the data or original file into multiple pieces called chunks and also needs to generate random coefficients. Then, it multiplies chunks with random coefficients and finally adds all resulting chunks before forwarding them to its neighbor. For a security protocol, if network coding is used instead of multicasting routing for data transmission, the network becomes more vulnerable for the attacker to confuse the data transmission [25–27].

A load balanced amortized multi-scheduling algorithm (LBAM) [28] is proposed for assigning the task to the cloud based on the active load in the cloud environment. This protocol calculates the cloud data weight based on the allocation of data and its significance based on the handling effectiveness of the cloud machine. This approach is used to ensure security between the data owner and the service provider in the cloud environment, which may not be the right approach for other public networks [29].

The proposed PDSCM protocol aspires to choose a secure forwarder in multicast communication with minimum computational overhead and less delay, as it uses orthogonal projection-based matrix computation to detect the malicious nodes in multicast wireless mesh networks.

3. Network Metrics

To discover the secure forwarder nodes from a source to the group of receivers, the proposed protocol uses two network metrics, viz., predictable delivery (P_D) ratio and ongoing delivery ratio (O_D). They are defined as follows.

3.1. Ongoing Delivery (O_D) Ratio

The node computes the ongoing delivery ratio for a path or link by calculating the current packet rate at which it receives data from its one-hop neighbor and it is estimated using the following Equation (1),

$$O_D = \frac{P_R}{P_S} \tag{1}$$

where P_R denotes the receiving packet count and P_S denotes the sending packet count from a source at the same time interval.

3.2. Predictable Delivery (P_D) Ratio

The predictable delivery ratio of a path or link is measured from continuous observations of each one-hop forwarding node for an expected packet delivery ratio.

4. Description of Data Forwarding Attack

The data forwarding attack in a multicast network is aimed to disrupt data transfer in a WMN. The impact of an attacker in the route discovery process is significant, as it can efficiently control the routes in the WMN. The strategy followed by an attacker is to announce false network metrics for routes to the sender, thereby creating the possibility of being selected as a forwarder node. A single malicious node may disturb communication to several receivers simultaneously; therefore, the effect of malicious nodes in a multicast scenario is considerably higher in comparison with their unicast environment. Hence, solving the security issues in a multicasting scenario is important.

Figure 1 shows the schematic representation of data-forwarding attacks in a multicast WMN. In Figure 1, the disruptive behavior of a vindictive node V_N is shown. The actual O_D metric value of a link ($S \rightarrow V_N$) from a source to V_N is 0.6; instead, V_N announces the false metric value of 0.9, so that S may choose V_N as an upstream forwarder for forwarding packets from source S to a set of multicast receivers (R). The vindictive node builds the link among the acquaintances as a neighbor and attempts to confuse the network transmissions between $S \rightarrow V_N$, so that the entire multicast transmission may collapse. In this article, the terms 'attacker' and 'vindictive' convey the same meaning of a malicious node.

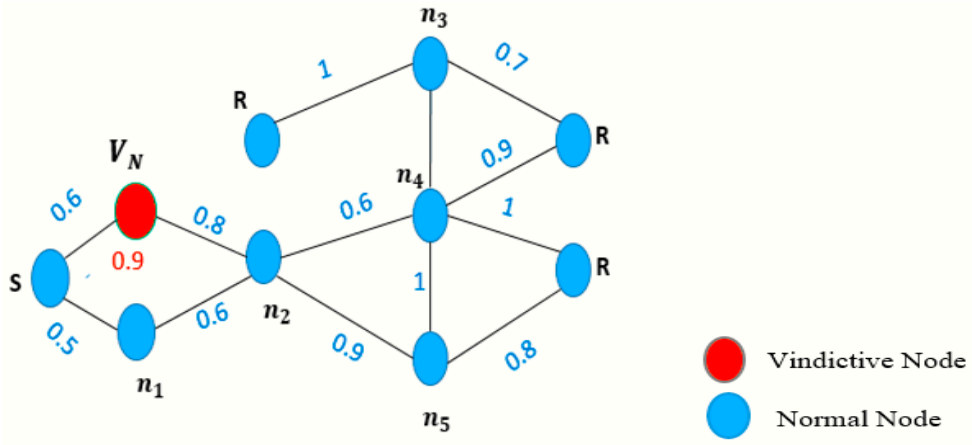


Figure 1. Schematic representation of data-forwarding attack in multicast WMN.

5. The Proposed PDSCM Protocol

This proposed protocol finds an optimal multicast route without a vindictive presence among acquaintances during the communication period. The statistical method is utilized

by constructing lower and upper bound estimates of the honest node's packet delivery ratio. Additionally, to ensure accuracy in identifying the behavior of a vindictive node, an orthogonal projection method is used. The network model used in this proposed PDSCM protocol is discussed in Section 5.1.

5.1. Network Model

The confidence of a WMN has been estimated and built as a network with a subjective graph in which $G = (N, E)$ and where $N = \{n_{1,} n_{2,} \ldots, n_k\}$ is characterized as the series of wireless nodes placed on the multicast-mesh network, and $E = \{(n_i, n_j)/i \neq j\}$ specifies the set of neighbors formed among the wireless mesh nodes. Each (n_i, n_j) is the direct neighbor between the n_i and n_j, at a specific time 't' with an explicit confidence level. For a particular node n_i, there may be several possible next-hop forwarder nodes to forward the data. If the number of the next-hop forwarder is more than one, then the secure next-hop forwarder known as a multicast router has to be nominated to forward the packets to the group of receivers. In such a scenario, the selection of next-hop forwarder is an important aspect in multicast routing.

5.2. PDSCM Algorithm

Algorithm 1 describes the proposed PDSCM algorithm. It consists of three phases, viz., the initialization phase, the path discovery phase, and the secure forwarder selection phase. They are discussed in the following Section 5.2, Section 5.3, and Section 5.4, respectively.

Algorithm 1 PDSCM algorithm to ensure secure next-hop forwarder in a multicast mesh network using PDSCM protocol.

Step 1: Input the network parameters.
I_P : *Initial parameter*, *allegation list*, L : *location_information*, C_C : *channel capacity*;
Step 2: If the next-hop neighbor is not in the *allegation list*, then the compute node's initial parameter
$node.I_P = L, C_C$;
Step 3: Compute P_D, O_D metrics
$O_D = \frac{P_R}{P_S}$
where P_D of a communication link is measured from continuous observations of each one-hop forwarding node for an expected packet delivery ratio.
Step 4: Perform secure forwarder node selection * as discussed in detail in *Section* 5.4.
Step 5: If a vindictive node is found, then add its node ID to the *allegation list*.
Step 6: Compute authentication signature for the accuser node using RSA encryption, which is used for signature generation and verification based on node ID along with the data packets.
Step 7: Send an allegation message in the network. The allegation message includes the node ID of both the accused node and the accuser along with the signature of the accuser.
Step 8: Perform signature verification for the accuser during the allegation message exchange.
Step 9: Upon successful validation of an allegation message, the accused nodes are marked as vindictive by adding a corresponding node entry to the allegation list, and the same node is removed from the current data transmission path.
Step 10: End.

5.3. Initialization Phase

During the initialization phase, every node in the mesh network constructs network metrics as mentioned in Section 3. The steps followed in this phase are described as follows.

1. Every node in the network shares the hello packet and builds the neighbor list to maintain the current neighbors periodically.
2. The initial next-hop forwarder selection is based on the initial parameter (I_P) metric, which is computed based on the location information (L) of the neighboring nodes and the channel capacity (C_c) of the wireless link from its neighbors to itself, as mentioned in PDSCM algorithm.

3. Every node in the network constructs a list of qualified forwarder nodes based on the I_P metric. Whenever communication takes place, the nodes compute the packet delivery capability of their neighboring nodes and measure P_D, O_D metrics periodically.
4. Each node maintains an allegation list that keeps vindictive information; consequently, the honest nodes eliminate the malicious nodes from the path, and the list gets updated periodically.
5. To ensure the authentication of nodes in the network, nodes share their signatures enclosed with their node ID along with the data packets. The authentication signature algorithm based on RSA is used for signature generation and verification.

5.4. Path Discovery Phase

The path discovery phase deals with two kinds of packets, viz., join request (JREQ) and join reply (JREP) packets, to find the best path from a source to a set of multicast receivers. The steps followed in this phase are described as follows.

1. If the source node wants to initiate a data transmission and does not have a path to reach the receivers, it broadcasts a JREQ message to a group of receivers.
2. The JREQ message contains various fields, viz., source address, multicast group address, Seqno, predictable delivery (P_D) ratio and ongoing delivery (O_D) ratio fields. The P_D and O_D fields are used to identify the sending and receiving packet ratio at each node. The forwarder node then sends the JREQ message to the group of receiver nodes.
3. When the set of receiver nodes receive JREQ messages, they verify the message sequence number to ensure the packet's freshness. If the sequence number is new, then the receivers send a JREP message to the source node through the forwarders based on the best (P_D, O_D) values recorded among the set of neighbor nodes, as its upstream node towards the source.
4. The JREP message contains the source address, multicast group address, REPID and return path information. The REPID is a unique ID to identify the JREP message and the return path information field contains path information to send the JREP message back to the source.
5. When the source node receives JREP message from the recipients, it then starts transmitting the data.

5.5. Secure Forwarder Selection Phase

The secure forwarder selection phase selects the secure forwarder by removing the vindictive nodes in the multicast path. Each honest node (normal node) in the network performs the following essential tasks, viz., vindictive boundary detection, orthogonal projection, and estimation, which are described in the subsequent Sections 5.5.1 and 5.5.2, respectively.

5.5.1. Vindictive Boundary Detection

The vindictive boundary detection task identifies every upstream vindictive node in the multicast path. The vindictive nodes are detected by constructing the confidence intervals that comprise the true range of values for the ongoing packet delivery (O_D) ratio. When the upstream forwarder node is suspected to be a vindictive node, then the confidence interval for that vindictive node is constructed. The strategy that has been followed for suspecting whether the node is vindictive or not is explained as follows.

Strategy for Identification of the Vindictive Node

When $P_D - O_D \geq \Delta$, (where 'Δ' is the detection threshold of packet dropping count considered from the maximum drop of the network), then the honest nodes suspect that the multicast path is under attack, as the path was unsuccessful in transporting the data packets at an expected speed according to the acknowledged excellence. Then, the honest node starts validating the node's security and trust by defining the following confidence

intervals for the detection of malicious nodes in the multicast path. The sample predictable and ongoing packet delivery ratio data is shown below in Table 1.

Table 1. Sample P_D and O_D data.

Channel/Link	P_D	O_D
8- > 5	1	0.701
32- > 5	1	0.673

Confidence Interval for the Detection of Malicious Nodes

For each upstream node n_j, the upper and lower limit interval for O_D is estimated using the statistical method by observing a number of O_D values over a period (every 0.1 sec) which may vary depending on the network size and traffic flows. A node can be declared as a malicious node if it does not satisfy the following inequality in Equation (2).

$$(X - \sigma) \leq O_D \leq (X + \sigma) \tag{2}$$

where $(X - \sigma)$ and$(X + \sigma)$ are described as a lower limit value and upper limit value for O_D.

Each node measures the packet receiving ratio (X) of its one-hop neighbors along with twin and quad unit values. The twin and quad unit values are based on the plus four rule to give an accurate estimate for a small number of samples and for extreme probability [14] and 'σ' is a corresponding standard deviation that is computed as shown below in Equation (3),

$$X = \frac{P_R + 2}{P_S + 4} \qquad \sigma = k\sqrt{\frac{X(1-X)}{P_S + 4}} \tag{3}$$

where P_R denotes the receiving packet count and P_S denotes the sending packet count from a source at the same time interval. Here, k = 1.95, to obtain the 95% confidence interval level for O_D. Table 2 shows the sample data of X, σ, lower and upper limit confidence interval of O_D.

Table 2. The sample data (X, σ, lower and upper limit confidence interval of O_D).

Link	X	σ	Lower Limit	Upper Limit
1- > 34	0.714286	0.334664	0.379622	1.04895

5.5.2. Orthogonal Projection and Estimation

In this section, the vindictive behavior of a node is identified accurately by using the orthogonal projection method. Specifically, the orthogonal projection method estimates whether the upstream node drops the received packets over successive time intervals.

Let n_i be a node that finds the next secure forwarder node among its one-hop neighbors, such as, $n_1, n_2, \ldots, n_k$. The proposed algorithm should determine the vindictive node among these one-hop neighbors of node n_i. To determine the vindictive behavior of a node n_j, consider a 2 × 2 matrix P_{n_j}, whose first row values are the O_D and P_D values of n_j, and whose second row values are the variance and standard deviation of n_j. The input matrix format and the sample input matrix to the orthogonal projection method are considered as shown below.

$$P_{n_j} = \begin{pmatrix} \boldsymbol{O_D} & \boldsymbol{P_D} \\ \boldsymbol{O_D'} & \boldsymbol{P_D'} \end{pmatrix} \quad P_{n_j} = \begin{pmatrix} 0.535 & 1 \\ 0.667 & 0.857 \end{pmatrix}$$

The orthogonal projection matrix D of the input matrix P_{n_j} is computed using the following steps as shown below.

Step 1. Compute transposition of P_{n_j}, which is denoted by ${P_{n_j}}^T$(4).
The output matrix is obtained based on Equation (4) as follows.

$$ {P_{n_j}}^T = \begin{pmatrix} 0.535 & 0.667 \\ 1 & 0.857 \end{pmatrix} \tag{4} $$

Step 2. Compute multiplication of matrices $\left(P_{n_j} {P_{n_j}}^T \right)$ and $\left({P_{n_j}}^T P_{n_j} \right)$ (5).
The resultant matrix based on Equation (5) is obtained as follows.

$$ P_{n_j} {P_{n_j}}^T = \begin{pmatrix} 1.287 & 1.214 \\ 1.214 & 1.800 \end{pmatrix} \quad {P_{n_j}}^T P_{n_j} = \begin{pmatrix} 0.732 & 1.107 \\ 1.107 & 1.734 \end{pmatrix} \tag{5} $$

Step 3. Compute $P'_{n_j} = I - \left(P_{n_j} {P_{n_j}}^T \right) \left({P_{n_j}}^T P_{n_j} \right)^{-1}$ (6),

where I is the 2×2 identity matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The resultant matrix P'_{n_j} is obtained based on Equation (6) as follows.

$$ P'_{n_j} = \begin{pmatrix} -19.249 & 12.227 \\ -2.565 & 1.6 \end{pmatrix} \tag{6} $$

Step 4. Compute $R = \left(P'_{n_j} \right)^T \left(P'_{n_j} \right)$ (7)
The output matrix obtained based on Equation (7) is as follows.

$$ R = \begin{pmatrix} 377.103 & -239.461 \\ -239.461 & 152.059 \end{pmatrix} \tag{7} $$

Step 5. Compute the inverse matrix R^{-1} (8).
The resultant inverse of a matrix R is obtained based on Equation (8) as follows.

$$ R^{-1} = \begin{pmatrix} 454.509 & 715.757 \\ 715.757 & 1127.174 \end{pmatrix} \tag{8} $$

Step 6. Compute the orthogonal projection matrix $D = \left(P'_{n_j} R^{-1} \right) {P'_{n_j}}^T$ (9).
The resultant orthogonal projection matrix obtained based on Equation (9) is as follows.

$$ D = \begin{pmatrix} 0.887 & -0.009 \\ -0.013 & 0.948 \end{pmatrix} \tag{9} $$

Step 7. Compute the final output matrix D_{t+1}, to obtain the orthogonal projection with the next iteration at time '$t + 1$' as follows in Equation (10),

$$ D_{t+1} = D\, P_{n_j} + P_{n_j} - D\, \overline{P_{n_j}} \tag{10} $$

where $\overline{P_{n_j}}$ is the standard packet delivery ratio of current upstream neighbor 'n_j' and that can be computed as follows in Equation (11).

$$ \overline{P_{n_j}} = \frac{1}{N} \sum_{i=1}^{N} P_{n_j} \tag{11} $$

The final projected matrix output obtained based on Equation (10) is shown below.

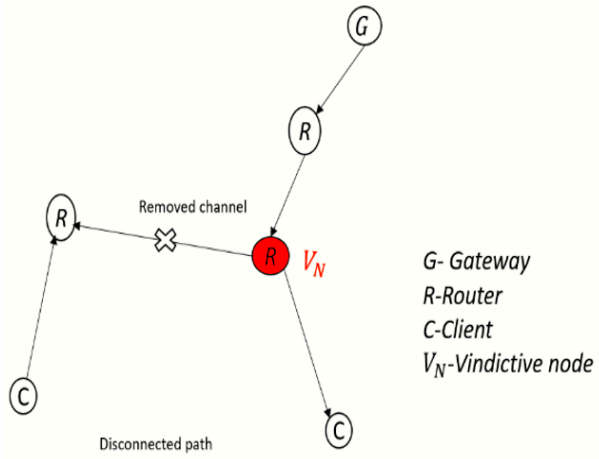
$$ D_{t+1} = \begin{pmatrix} 0.797 & 1.393 \\ 0.667 & 0.923 \end{pmatrix} \tag{12} $$

Using an orthogonal projection algorithm, every node estimates whether its upstream forwarder node drops the received packets over successive time intervals. The above Equation (10) in step 7 is computed repeatedly for every one-hop upstream neighbor for n iterations to observe the behavior of malicious nodes. After n^{th} iteration, by validating the final projection value with the boundary limitation based on Equation (2), the O_D values that are bounded outside of the normal node ranges are marked as vindictive values. Finally, the honest accuser node (a node that accuses the vindictive node) declares the corresponding upstream forwarder node as a malicious node as per the computed knowledge. Therefore, the malicious node is declared as a vindictive node by broadcasting an allegation message in the network. Figure 2 shows the format of an allegation message.

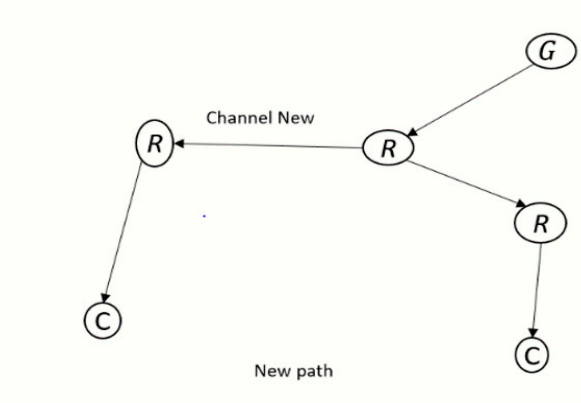
Allegation message			
Multicast group address	Accuser-node ID	vindictive-node ID	signature of the accuser

Figure 2. Allegation message.

An allegation message includes the node ID of both accused node and the accuser along with the signature of the accuser. The signature verification is performed for the accuser during the allegation message exchange. Upon successful validation of an allegation message, a charged node is marked as vindictive by adding a corresponding node entry to its allegation list and the same node is removed from the current data transmission path as shown in Figure 3a (detection of vindictive node) and Figure 3b (removal of vindictive node).



(**a**)



(**b**)

Figure 3. (**a**) Detection of vindictive node; (**b**) removal of vindictive node.

The behavior of the vindictive marked node in the current allegation list is again validated based on the estimation $P_D - O_D \geq \Delta$, until the end of the communication to confine the vindictive node, so that the vindictive marked node is permanently removed from the neighbor list and subsequently from the network itself.

6. Results and Discussion

The PDSCM protocol was simulated using Network Simulator Version 2 (NS-2) and the data packets of constant bit rate (CBR) were transmitted from a sender to the group of receivers. The number of clients and routers increased depending on the needs of the network. The nodes exchanged their locations using the random waypoint model and the network was built within a network area of 800 × 800 square meters with 100 nodes. During the communication, each node began its data transmission through the forwarder securely to reach the group of destinations. Once the multicast group was created according to the PDSCM method, the data packets were moved to the multicast path. This route-building process was repeated throughout the simulation. The simulation parameters used in the network are shown in Table 3.

Table 3. Simulation parameters—PDSCM.

Parameter	Value
Radio-propagation model	Random waypoint model
MAC type	Mac/802_11
Antenna model	Antenna/omni antenna
Routing protocol	PDSCM
Simulation area	800 × 800 square meters
Nodes	100
Initial energy in joules	100
Data packet size	512 bytes
Receiving power	0.6 W
Transmission power	0.9 W
Traffic type	CBR
Simulation time	200 s

The proposed protocol was evaluated by comparing its performance with existing multicast protocols: the efficient fuzzy-based multi-constraint multicast routing protocol (EFMMRP) [2] and multi-criteria routing metric (MCR) for supporting data-differentiated service [19], the ODMRP protocol using a high-throughput metric (ODMRP-HT) [17], the secure multicast routing algorithm for wireless mesh network (SEMRAW) [18], rank-based forwarder selection in multicasting with fuzzy optimized path formation (RFSMPF) [1], and energy saving slot allocation-based multicast routing (ESAM) [20] using the following network performance metrics, viz., packet-received count, packet delivery ratio, throughput, and packet delivery delay.

It can be observed in Figure 4 that the average number of packets received by the multicast receivers under various time intervals was higher in PDSCM compared to that of existing multicast protocols, as the multicast packets were securely delivered in the mesh network. Due to accurate design and secured forwarder selection during the route discovery process, the proposed protocol achieved a better outcome. In addition, since the PDSCM protocol is a preventive-based approach, the packet received count was high. Hence, the network did not suffer from initial packet losses until the finding of malicious nodes, and the packet received count of the proposed protocol was higher than those of compared protocols. It outperformed EFMMRP by 57.1%, MCR by 41.8%, RFSMPF by 24.1%, and ESAM by 18.4%.

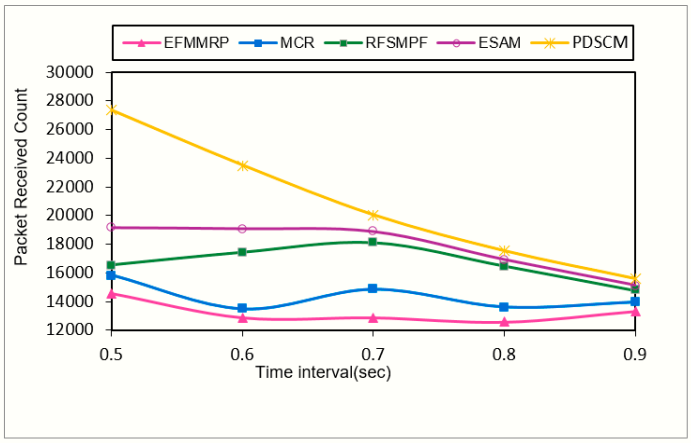


Figure 4. Packets received count vs. time interval.

Figure 5 shows the packet delivery ratio by varying the number of nodes from 10 to 70 in a wireless mesh network. When there is a huge number of nodes in a network, there are more possibilities to create a secure multicast routing path that leads to fewer opportunities for packet loss. Once the packets were transmitted from a source to a set of receivers, the PDSCM ensured that packets were forwarded only through honest nodes, which avoided huge packet losses in the network. Due to accurate vindictive node elimination, the proposed technique attained the highest packet delivery ratio compared to existing multicast protocols. The PDSCM outperformed the existing approaches with a PDR of 98.1%, outperforming EFMMRP by 15.4%, MCR by 19.6%, RFSMPF by 8%, and ESAM by 5.2%.

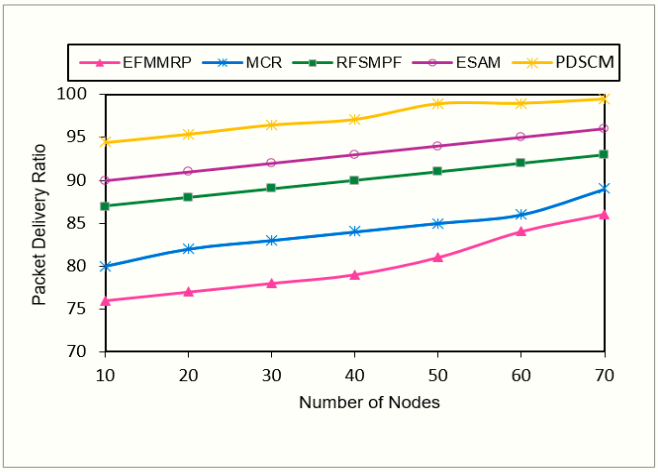


Figure 5. Packet delivery ratio vs. number of nodes.

Figure 6 shows that the throughput of the network increased steadily when the network size increased over successive intervals. Due to secure forwarder node selection, the packet arrival time was reduced. In addition, as every node's communication behavior was analyzed based on its packet deliverance capability and on current network environmental variations promptly, the vindictive nodes were accurately identified and removed from the network. This increased network throughput. The proposed PDSCM protocol had better throughput than existing protocols, viz., outperforming EFMMRP by 11.6%, MCR by 8.4%, RFSMPF by 4%, and ESAM by 2.2%.

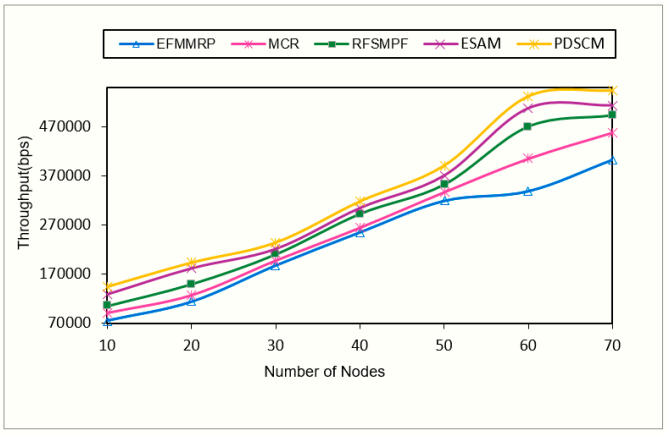


Figure 6. Throughput vs. number of nodes.

It can be observed from Figure 7 that packet delivery delay increased slowly as the number of nodes increased. The proposed protocol outperformed the existing protocols by reporting an average packet delivery delay of 0.06 s when the number of nodes increased gradually. The vindictive node elimination from the communication path ensured a minimum end-to-end delay path that sent the highest bits per second to the receivers. Hence, the packet delivery time was greatly reduced in PDSCM. On an average, PDSCM incurred less delay than existing protocols, outperforming EFMMRP by 76%, MCR by 72%, RFSMPF by 70%, and ESAM by 40%.

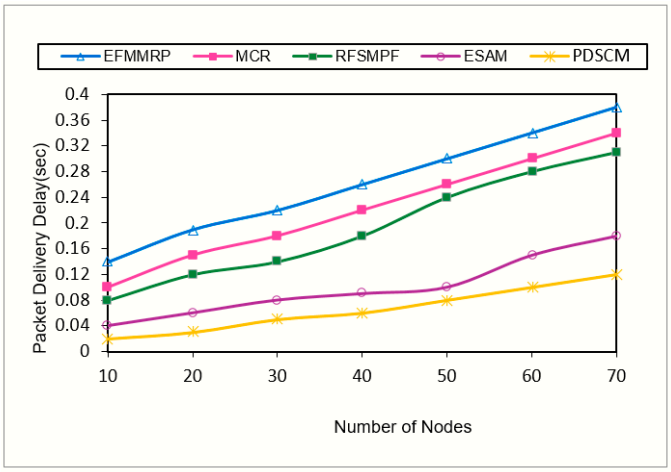


Figure 7. Packet delivery delay vs. number of nodes.

Figure 7 shows the performance comparison of PDSCM with a varying number of malicious nodes, in terms of the percentage of packets delivered. From Figure 8, it can be observed that as the number of malicious nodes increased, there was a sudden decrease in the packet delivery ratio (when the number of a malicious nodes reached 20, the PDR decreased from 98% to 96%). This is because as the number of malicious nodes increases, some multicast receivers become completely inaccessible and they are not able to receive data. The proposed protocol showed better results than the conventional secure multicast protocols, viz., ODMRP-HT and SEMRAW.

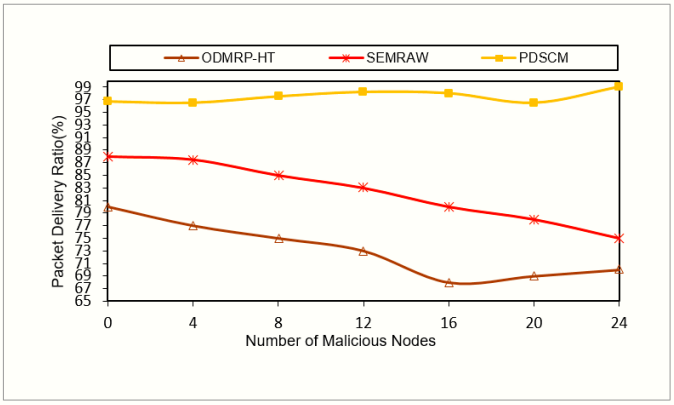


Figure 8. Packet delivery ratio vs. number of malicious nodes.

7. Conclusions

The proposed PDSCM protocol is a mesh-based secure multicast routing protocol designed with secured forwarder selection and path selection. It has been found that the proposed PDSCM protocol outperforms the existing protocols on various performance metrics. Additionally, the twin and quad unit computations on the packet delivery ratio and orthogonal projection-based computations provided multi-dimensional results to finalize the forwarder nodes without malicious characteristics in the multicast mesh group. Multi-agent systems were recently developed in response to the rising demand for distributed problem solving. This work can be further extended to secure the mobile agent platforms in ubiquitous computing applications and systems.

Author Contributions: Conceptualization, S.S. and E.D.; methodology, S.D. and A.J.; validation, A.J. and J.E.R.; writing—original draft preparation, S.S., E.D. and S.D.; writing—review and editing, A.J. and J.E.R.; visualization, J.E.R.; supervision, A.J. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data is available on request to the authors.

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

References

1. Khadmaoui-Bichouna, M.; Alcaraz-Calero, J.M.; Wang, Q. Empirical evaluation of 5G and Wi-Fi mesh interworking for Integrated Access and Backhaul networking paradigm. *Comput. Commun.* **2023**, *209*, 429–443. [CrossRef]
2. Quy, V.K.; Chehri, A.; Quy, N.M.; Han, N.D.; Ban, N.T. Innovative Trends in the 6G Era: A Comprehensive Survey of Architecture, Applications, Technologies, and Chal-lenges. *IEEE Access* **2023**, *11*, 39824–39844. [CrossRef]
3. Nouri, N.A.; Aliouat, Z.; Naouri, A.; Hassak, S.A. Accelerated PSO algorithm applied to clients coverage and routers connectivity in wireless mesh net-works. *J. Ambient. Intell. Humaniz. Comput.* **2023**, *14*, 207–221. [CrossRef]
4. Seetha, S.; Anand, J.F.S.; Kanaga, E.G.M. RFSMPF: Rank based forwarder selection in MCAST with fuzzy optimized path formation in wireless mesh network. *Wirel. Netw.* **2019**, *25*, 4287–4298. [CrossRef]
5. Hu, H.; Ye, M.; Zhao, C.; Jiang, Q.; Wang, Y.; Qiu, H.; Deng, X. Intelligent multicast routing method based on multi-agent deep reinforcement learning in SDWN. *arXiv* **2023**, arXiv:2305.10440. [CrossRef]
6. Yadav, A.K.; Das, S.K.; Tripathi, S. EFMMRP: Design of efficient fuzzy based multi-constraint multicast rout-ing protocol for wireless ad-hoc network. *Comput. Netw.* **2017**, *118*, 15–23. [CrossRef]
7. Murugeswari, R.; Devaraj, D. Multiconstrained QoS Multicast Routing for Wireless Mesh Network Using Discrete Particle Swarm Optimization. In *Artificial Intelligence and Evolutionary Computations in Engineering Systems: Proceedings of ICAIECES 2016*; Springer: Singapore, 2017; pp. 847–859.
8. Gupta, B.K.; Patnaik, S.; Nayak, A.K.; Mallick, M.K. Congestion managed multicast routing in wireless mesh network. *Int. J. Commun. Netw. Inf. Secur.* **2017**, *9*, 484–490. [CrossRef]

9. Ibraheem, I.K.; Al-Hussainy, A.A.-H. A multi QoS genetic-based adaptive routing in wireless mesh net-works with Pareto solutions. *arXiv* **2018**, arXiv:1805.00973.
10. Rao, A.N.; Rao, C.D.V.S. Way-point multicast routing framework for improving QoS in hybrid wireless mesh net-works. *Wirel. Netw.* **2016**, *22*, 2681–2694.
11. Meraihi, Y.; Acheli, D.; Ramdane-Cherif, A. QoS multicast routing for wireless mesh network based on a modified bi-nary bat algorithm. *Neural Comput. Appl.* **2019**, *31*, 3057–3073. [CrossRef]
12. Duchamp, G. Orthogonal projection onto the free Lie algebra. *Theor. Comput. Sci.* **1991**, *79*, 227–239. [CrossRef]
13. Dan, M.; Rabinoff, J.; Rolen, L. *Interactive Linear Algebra*; Georgia Institute of Technology: Atlanta, GA, USA, 2017.
14. Wallis, S. Binomial confidence intervals and contingency tests: Mathematical fundamentals and the evaluation of alternative methods. *J. Quant. Linguist.* **2013**, *20*, 178–208. [CrossRef]
15. David, S.M.; Notz, W.I.; Fligner, M.A. *The Basic Practice of Statistics*; Macmillan Higher Education: New York, NY, USA, 2015.
16. Seetha, S.; Francis, S.A.J. Secure Multicasting Protocols in Wireless Mesh Networks—A Survey. In *Computational Intelligence, Cyber Security and Computational Models: Proceedings of ICC3, 2013*; Springer: New Delhi, India, 2014; pp. 245–256.
17. Li, Y.; Ray, C. Hierarchical agent-based secure multicast for wireless mesh networks. In Proceedings of the 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 5–9 June 2011; IEEE: New York, NY, USA, 2011; pp. 1–6.
18. Shin, S.; Hur, J.; Lee, H.; Yoon, H. Bandwidth efficient key distribution for secure multicast in dynamic wireless mesh networks. In Proceedings of the 2009 IEEE Wireless Communications and Networking Conference, Budapest, Hungary, 5–8 April 2009; IEEE: New York, NY, USA, 2009; pp. 1–6.
19. Kim, J.; Bahk, S. Design of certification authority using secret redistribution and multicast routing in wireless mesh networks. *Comput. Netw.* **2009**, *53*, 98–109. [CrossRef]
20. Dong, J.; Ackermann, K.; Nita-Rotaru, C. Secure group communication in wireless mesh networks. *Ad Hoc Netw.* **2009**, *7*, 1563–1576. [CrossRef]
21. Balaji, S.; Sasilatha, T. Secure on demand multicast routing for network attacks in wireless mesh network. In *Proceedings of the International Conference for Phoenixes on Emerging Current Trends in Engineering and Management (PECTEAM 2018)*; Atlantis Press: Paris, France, 2018; pp. 20–23.
22. Matam, R.; Tripathy, S. Secure multicast routing algorithm for wireless mesh networks. *J. Comput. Netw. Commun.* **2016**, *2016*, 1563464. [CrossRef]
23. Sharma, B.; Vaid, R. Efficient Key Management for Secure Communication Within Tree and Mesh-Based Multicast Routing Protocols. In *Mobile Radio Communications and 5G Networks: Proceedings of Second MRCN 2021*; Springer Nature: Singapore, 2022; pp. 501–510.
24. Sharma, B.; Vaid, R. A Secure Key Management on ODMRP in Mesh-Based Multicast Network. In *Computational Intelligence for Engineering and Management Applications: Select Proceedings of CIEMA 2022*; Springer Nature: Singapore, 2023; pp. 521–530.
25. Dong, J.; Curtmola, R.; Nita-Rotaru, C. Secure network coding for wireless mesh networks: Threats, challenges, and directions. *Comput. Commun.* **2009**, *32*, 1790–1801. [CrossRef]
26. Anwar, A.L.H.; Barakat, C.; Turletti, T. Network coding for wireless mesh networks: A case study. In Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06), Buffalo-Niagara Falls, NY, USA, 26–29 June 2006; IEEE: New York, NY, USA, 2006; p. 9.
27. Chen, P.; Shi, L.; Fang, Y.; Lau, F.C.M.; Cheng, J. Rate-diverse multiple access over Gaussian channels. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 5399–5413. [CrossRef]
28. Jeyakarthic, M.; Subalakshmi, N. Energy saving slot allocation-based multicast routing in cloud wireless mesh net-work. *Int. J. Cloud Comput.* **2023**, *12*, 148–162. [CrossRef]
29. Fathima, M.A.; Munsifa, A.F. Mobile agent platforms in ubiquitous computing applications and systems (a literature review). In Proceedings of the 6th International Symposium, Heidelberg, Germany, 11–15 July 2016.