Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7240795, 20 pages
https://doi.org/10.1155/2022/7240795

*Research Article*

# Efficient Key Management Mechanism with Trusted Gateways for Wireless Mesh Networks

**Ganesh Reddy Karri**,[1] **A. V. Prabu**,[2] **Sidheswar Routray**,[3] **D. Sumathi**,[1] **S. Rajasoundaran**,[4] **Amrit Mukherjee**,[5] **Pushpita Chatterjee**,[6] **and Waleed Alnumay**[7]

[1]*School of Computer Science and Engineering, VIT AP University, India*
[2]*Department of Electronics and Communication Engineering, Koneru Lakshmaiah Education Foundation, Guntur, India*
[3]*Department of Computer Science and Engineering, School of Engineering, Indrashil University, Rajpur, Mehsana, Gujarat, India*
[4]*School of Computing Science and Engineering, VIT Bhopal University, Bhopal, India*
[5]*Department of Computer Science, Faculty of Science, University of South Bohemia in Ceske Budejovice, Czech Republic*
[6]*Tennessee State University, Nashville, USA*
[7]*Department of Computer Science, Riyadh Community College, King Saud University, P.O. Box 2455, Riyadh 11451, Saudi Arabia*

Correspondence should be addressed to Sidheswar Routray; sidheswar69@gmail.com and Amrit Mukherjee; amrit1460@ieee.org

Received 18 March 2022; Revised 16 June 2022; Accepted 20 July 2022; Published 17 August 2022

Academic Editor: A.H. Alamoodi



Securing wireless mesh networks (WMNs) is a crucial issue due to its intrinsic characteristics. Several endangered features might emerge due to the exposure of the networks to a diversity of medium access control (MAC) layers such as distributed denial of service (DDoS) attacks, false reply attacks, and other identity attacks. Against these attacks, the determination of existing techniques is insufficient to ensure the complete security solutions to protect the backbone network at multiple levels. As a result, effective, scalable, and integrated security solutions for WMNs are required. In WMNs, protecting legitimate gateway nodes and internal mesh routers against malicious attacks at the MAC layer remains a difficult problem. Our proposed trust-based security mechanism includes distributed authentication and deauthentication algorithms that validates backbone mesh routers as well as gateway nodes. Particularly, this proposed model targets DDoS attacks in the network. The proposed DDoS attack prevention mechanism (DAPM) uses distributed authentication and deauthentication algorithms to build trusted group heads for managing secure data communication in the network. Our research and practical results show that the proposed mechanism decreases the severity of malicious nodes and strengthens the security compared to existing centralized schemes such as digital signature authentication (DSA-Mesh, MENSA, Mobisec, and AHKM). The experimental solutions show the significance of the proposed work with 10% to 12% of better performance than the existing techniques.

## 1. Introduction

Nowadays, wireless mesh network (WMN) technologies such as 802.11 s, 802.15, 802.16 (WiMAX), and 802.20 have evolved widely in the wireless arena [1–4]. In this case, multihop client mesh architecture, distributed server authentication, and other sophisticated capabilities are still expected in the IEEE 802.16 standard.

In this domain, the existing standards have only a limited impact on the scalability and availability of a network's infrastructure since they only address a subset of WMN features. The available techniques are still in the early stages of development as they are reliant on wireless standards [5, 6]. WMNs have various security issues that must be addressed with compatibility and integration. The basic design of WMN is shown in Figure 1(a). As we discussed, protection of the legitimate nodes from the adversary nodes at the MAC layer of mesh networks is a tough task [6]. We split critical management solutions into two groups such as centralized systems and distributed systems to secure the data from the adversaries. The communication overhead and unreliable qualities of centralized key management

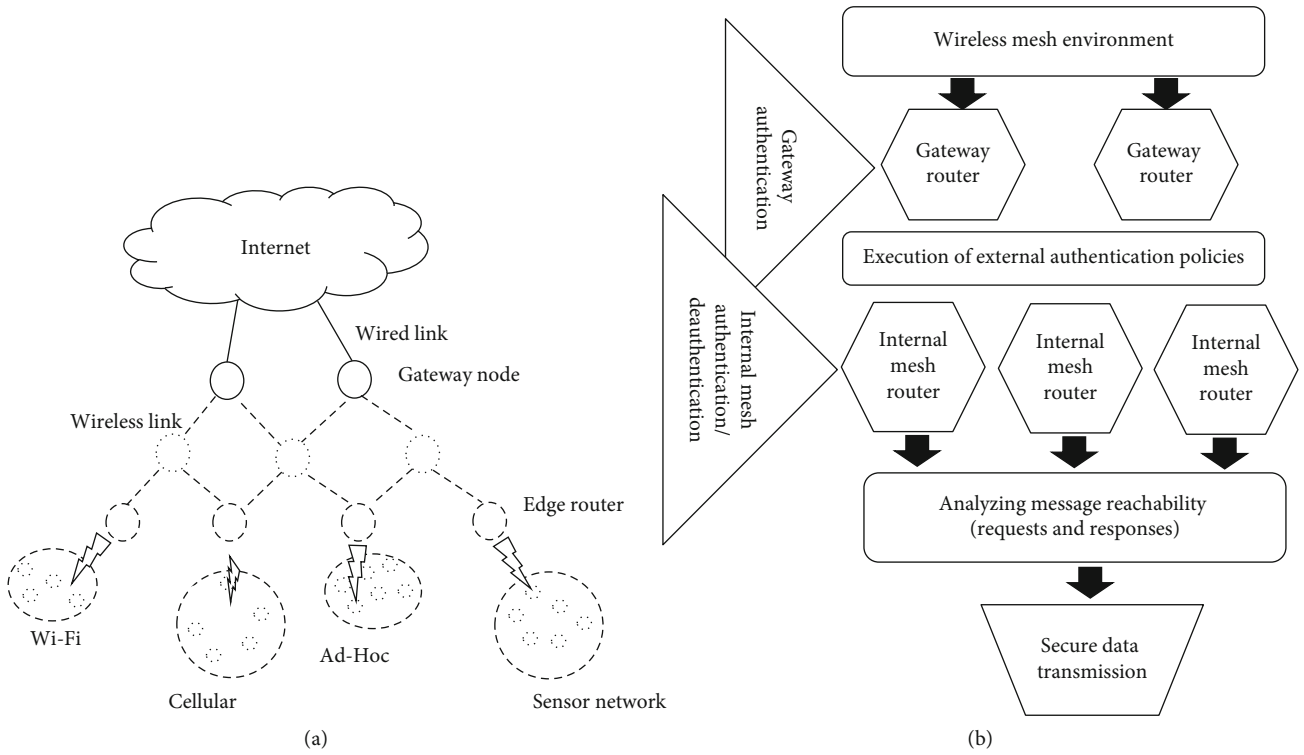



Figure 1: (a) WMN architecture. (b) Proposed DAPM for WMN authentication policies.

technologies like adaptive key management (AKHM) and Mobisec can be linked to their ineffectiveness. The fault-tolerance of approaches like DSA-Mesh and the IEEE 802.16j multihop relay security architecture does not protect unicast and broadcast communications from MAC layer attacks in these systems.

Multilevel key management mechanisms have recently been included to make key distribution easier. On a variety of levels, these solutions are ineffective to address the security issues connected with the backbone mesh. In this connection, WMNs are expected to use multilevel key management mechanisms to protect legitimate mesh nodes from rogue nodes in order to work with stability [7]. Particularly, the development of a multilevel key management mechanism, distributed public key authentication, deauthentication procedures, and confidentiality management in group leaders is employed to protect legal mesh nodes in WMNs. This practice creates a possibility to make effective use of the trustworthy group heads for secure data communication in WMNs.

Against unauthorized access, suitable authentication systems are required for WMNs. The cooperative DDoS attacks can harm the network to isolate legitimate mesh nodes from WMNs. Malicious attackers cooperate in this scenario to isolate genuine mesh nodes by prohibiting them from exchanging data or authentication request messages. Since there are no distributed key management processes, DDoS attacks have a significant impact on the backbone mesh. As a result of this requirement, the need for a distributed key management solution to protect against backbone mesh DDoS attacks has evolved.

Security for heterogeneous devices with backbone mesh allows communication with each other and access. WMNs typically use a two-tier key distribution scheme, with the gateway and router serving as the primary distribution points. The primary work of two-level distributed architecture is deploying stable gateways and nodes. Mesh routers are less mobile than regular routers, and gateways must authorize these nodes on a second level before they can operate. Existing security measures are designed to address security vulnerabilities at the gateway or router level. As a result, WMN's two-tiered design is vulnerable to various DDoS attacks. To secure genuine mesh nodes, mesh networks must incorporate a comprehensive two-level security key management approach, which is currently lacking in the present mechanisms.

The novelty of the proposed work lies in the successful authentication of the internal mesh router point and gateway point. The contributions of the proposed work are listed below.

(i) Gateway router authentication

(ii) Distributed node authentication

(iii) Dual authentication procedures against cooperative DDoS

(iv) Providing distributed perimeter security in WMN

According to the major contributions listed above, the proposed system ensures multilayered authentication and deauthentication principles at different network levels. Particularly, the novel authentication principles are executed against DDoS attacks through the transmission of both route requests and route replies around the distributed WMNs. In

addition, this proposed model supports the maximum reachability rate through data transmission and data reception. Under this experiment, the proposed security model has gateway authentication principles and internal router authentication principles to raise protection against DDoS attacks. Accordingly, the proposed mechanism gives efficient attack protections against both internal malfunctions and external malfunctions. This novel practice ensures overall distributed perimeter security against DDoS attacks (internal/external) in the complicated WMNs.

The remaining sections of this article are organized as follows. Section 2 describes the notable works of various literature. DAPM and the technical features are presented in Section 3. Section 4 discusses the performance of DAPM in WMNs. Section 5 concludes this paper.

## 2. Related Works

This section describes the existing centralized and distributed key architectures in WMNs. Dong et al. [8] suggested a Mobisec security architecture in which the public and private key pairs are distributed to newly joined routers by a centralized key distribution server.

In this framework, a new router prepares a signed authentication request and broadcasts it to nearby routers after validating the request. The neighboring router rebroadcasts the request if it is valid, and the procedure is repeated by intermediate routers until the request reaches the server. The server transmits the symmetric key as a reply to a new router for secure communication once the signed request message is valid. This work proposed the SeGroM architecture for WMNs. The SeGroM architecture uses a centralized key distribution approach and places the mesh nodes in a hierarchical tree structure. The mesh nodes are classified into two types, such as gateways and routers. The gateway node is the trusted node for all one-hop connected downstream mesh nodes and issues the keys to each downstream group node for secure link communication [9–11].

In this approach, control overhead is minimum since each gateway (group head) issues the keys only to downstream mesh routers instead of issuing the keys to both upstream and downstream members. The wireless standard 802.11i has a centralized key distribution architecture that secures the communication between the mesh clients and a mesh router [12]. Based on this work, the mesh router and mesh client use a four-way handshake to set up the Pairwise Transient Key (PTK) for secure link communication and the Group Wise Transient Key (GTK) for establishing a secure group communication. The wireless standard 802.11 s has centralized key distribution architecture for securing multihop communication in WMN.

Based on the security features of 802.11 s, mesh nodes are classified into three types, such as mesh key distributor (MKD), supplicant, and mesh authenticator (MA) [13]. MA nodes are successfully authenticated by the authentication server, and they can forward the authentication request messages of a supplicant (new mesh router) node to an MKD node when the supplicant does not have a direct link to the MKD. The MKD node replies to the supplicant through the MA node. The MA node and supplicant node use a four-way handshake protocol for the secure exchange of the PTK and GTK. Theil et al. proposed a hybrid wireless mesh network distributed security architecture [14]. In this security architecture, IEEE 802.11w protects the communication between the mesh points [15], and an enhanced four-way authentication protocol (IEEE 802.11i) is used to create the shared symmetric key between the access point and the mesh point.

Under this circumstance, the management frame protection of IEEE 802.11w provides end-to-end data secrecy between mesh points, and a shared symmetric key provides data confidentiality between the mesh point and the access point. To keep data safe in the path under hybrid wireless mesh networks, both mesh point security and access point security are required. DSA-Mesh has a distributed security key architecture that protects the backbone mesh networks' general routes and core routers. Core routers choose the peer master node in this design, and this node's job is to broadcast the request message and generate the session key from the random integers chosen by other core routers. The peer master node establishes a session key and broadcasts it to core routers after receiving reply messages from preceding routers. The session key encrypts the general router's joining request message. As a result, the general router sends a decryption request message to all core routers. The generic router waits for a minimum of $t$ reply messages from the source.

Praveen et al. presented an authentication security architecture to protect the cloned AP from internal attackers. The new joining access point (AP) broadcasts the MAC details as a request message in this process [16, 17]. Consequently, the gateway node checks these details in the existing database after receiving this request. Once the details of the AP are already contained in the database, the gateway node assumes the request message is from a cloned AP. Otherwise, the gateway node saves these details in a database and sends join AP information to its network nodes through broadcast.

Similarly, the recent works mainly identify various types of attacks and counter solutions in wireless networks [18–20]. Gayatri et al. [21] and Kasirajan et al. [22] proposed trust-based feedback routing and authentication mechanisms in wireless networks. Similarly, Soundararajan et al. [23] proposed secure watchdog mechanisms in wireless sensor networks. Most of the recent works are hardly trying to secure distributed wireless medium using either centralized solutions or distributed solutions. These works are mainly using lightweight distributed authentication and confidentiality procedures. Anyhow, the need for an optimal dual authentication mechanism is important against cooperative DDoS attacks in WMN [24, 25]. The lack of suitable authentication mechanisms against DDoS attacks at gateways and distributed nodes are considered a major research problem. This article is motivated to build resilient two-way authentication mechanisms against the current security issues.

## 3. DDoS Attack Prevention Mechanism (DAPM)

Our proposed DAPM uses two levels of authentication, such as gateway level authentication and router level authentication,

to protect legitimate routers. In DAPM, distributed authentication and deauthentication algorithms make use of gateway nodes as trust nodes. These gateway nodes are specialized routers that have very minimal resource constraints. The implementation of the gateway-level trust has been discussed in Section 3.2. These nodes use the WMN's authentication and deauthentication algorithms that have been discussed in Section 3.3 to ensure that mesh routers can connect securely to the network [26, 27].

*3.1. DAPM.* The descriptions of DAPM notations are shown in Table 1. Table 1 illustrates the trusted gateway nodes, as $\{g_i\}_{\{i=1,\cdots,|G|\}}$, where $g_i$ represents the $i^{\text{th}}$ gateway node. Each gateway node $(g_i)$ creates a digital signature on the messages $(\{M\}_{K_{g_i}^{-1}})$ with its private key $(K_{g_i}^{-1})$ and other network nodes. In this case, the gateway node $(g_i)$ with public key $(K_{g_i})$ uses to verify the messages. Mesh routers are represented as $R = \{r_{i,j}\}_{i=1,\cdots,|G| \text{ and } j=1,\cdots,|R|}$, where $j$ is a router id which belongs to $i^{\text{th}}$ gateway. The neighboring mesh routers are represented as $(\text{RN} = \{rn_{i,j}\}_{\{i=1,\cdots,|G'| \text{ and } j=1,\cdots,|R'|\}})$, where $j$ is a neighboring mesh router id belongs to $i^{\text{th}}$ gateway and $G'$ and $R'$ are other network nodes. Mesh router provides secure communication using its public key $(K_{r_{i,j}})$ and private key $(K_{r_{i,j}}^{-1})$. Each mesh router maintains router and gateway ids and their public keys in the authentication table $(\text{AT}_{i,j})$. The gateway maintains all authenticated router and gateway ids and their key pairs in the gateway authentication table $(\text{AT}_i)$.

Every new mesh router receives a unique router id from the gateway node $(g_i)$, as well as Advanced Encryption Standard- (AES-) 128 bit session key $(S_{K_{i,j}})$ for secure communication between the gateway and the mesh router. Gateway node issues the timeout interval $(T_{i,j})$ to the new router. The new router must join in the backbone mesh during this $T_{i,j}$ period. Gateway also issues maximum waiting time $(T_{i,j}^{\max})$ of a router to get the reply message from the gateway for the corresponding request packet.

$\text{ARQ}_{i,j}$ messages are sent by the router to join the backbone mesh. $\text{DARQ}_{i,j}$ messages are transferred by the router to leave the backbone mesh. Mesh router authentication replies $(\text{ARP}_{i,j})$ and deauthentication responses $(\text{DARP}_{i,j})$ are generated by the gateway in response to the successful authentication and deauthentication of the router. Routers and gateways use the number of node disjoint paths $(t_d)$ with the minimal degree of gateway $(g_i)$ to forward the authentication request $(\text{ARQ}_{i,j})$ and deauthentication request $(\text{DARQ}_{i,j})$. A mesh router $(r_{i,j})$ creates the collision-free one-way hash function $(H(M)_{S_{K_{i,j}}})$ for message integrity check using its session key $(S_{K_{i,j}})$.

*3.2. Gateway-Level Trust.* In the backbone mesh, gateway nodes or group heads trust each other via a traditional wired network. Due to the availability of industry-standard security methods, wired networks are more secure than wireless medium. In this work, the mutual authentication between group heads is considered using the standard wired security protocol (IPsec). Likewise, group heads provide the security of the backbone mesh by providing authentication, confidentiality, integrity, and nonrepudiation to each router using IPsec in the network. By signing group head signatures, each group head $(g_i)$ verifies their corresponding router request messages and shares the updated authentication table $((\text{AT}_i)_{K_{g_i}})$ with other group heads. Finally, gateway nodes authenticate with the corresponding group head's public key $(K_{g_i})$.

As given in Figure 1(b), the entire DAPM functions are illustrated with crucial multilayered authentication principles. As mentioned, WMNs are constructed with the help of both gateways and internal routers (neighbors). Gateway routers are responsible for analyzing the external and internal network traffics. At the same time, the internal routers or other forwarding nodes are vulnerable to get internal malicious events. The proposed model is implemented to set authentication and identity evaluation mechanisms at both gateway points and internal points. On this basis, the proposed model establishes distributed authentication rules for transmitting requests and responses. This approach detects reply attacks, DDoS attacks, and other authentication attacks and isolates the malicious events in the entire WMN at both gateways and internal routers.

Table 1: Distributed authentication scheme notations.

| | |
|---|---|
| $G$ | Set of trusted gateway nodes $\{g_1, g_2, g_3, \cdots, g_n\}$ |
| $g_i$ | $i^{\text{th}}$ gateway node |
| $K_{g_i}$ and $K_{g_i}^{-1}$ | Public and private key pair of $gw_n$ |
| $\{M\}_{K_{g_i}^{-1}}$ | Message singed by $g_i$ |
| $R$ | Mesh routers |
| $r_{i,j}$ | $j^{\text{th}}$ mesh router belongs to $g_i$ |
| RN | Neighboring mesh routers |
| $rn_{i,j}$ | $j^{\text{th}}$ neighboring router for $r_{i,j}$ |
| $K_{r_{i,j}}$ and $K_{r_{i,j}}^{-1}$ | Public and private key pair of $r_{i,j}$ |
| $\text{AT}_{i,j}$ and $\text{AT}_i$ | Authentication information table of $r_{i,j}$ and $g_i$ |
| id | Mesh router key identifier |
| $S_{K_{i,j}}$ | AES-128 bit session key |
| $T_{i,j}$ | New router $r_{i,j}$ timeout interval |
| $T_i^{\max}$ | Maximum waiting time of $g_i$ members |
| $\text{ARQ}_{i,j}$ | Authentication request of $r_{i,j}$ |
| $\text{DARQ}_{i,j}$ | Deauthentication request of $r_{i,j}$ |
| $\text{ARP}_{i,j}$ | $g_i$ authentication reply for $r_{i,j}$ |
| $\text{DARP}_{i,j}$ | $g_i$ deauthentication reply for $r_{i,j}$ |
| $t_d$ | Node disjoint paths |
| $H(M')_{S_{K_{i,j}}}$ | Collision free one-way hash function (key uses) |

In this security framework, forwarding nodes and gateway nodes execute authentication and deauthentication principles under the distributed scenario. The continuous security management principles ensure node authentication policies and path authentication policies. Thus, the entire WMN is protected under the secure circumstance. The technical characteristics and algorithms are illustrated in detail in the following sections.

*3.3. Authentication and Deauthentication at Router Level.* The proposed work uses authentication and deauthentication algorithms to secure mesh router's connection establishment rules. In mesh router authentication, group head $g_i$ issues the signed unique router-id ($\{\mathrm{id}\}_{K_{g_i}^{-1}}$) to every new router ($r_{i,j}$). Before joining the group, a new mesh router ($r_{i,j}$) sends a request message for the validation of its signed router-id ($\{\mathrm{id}\}_{K_{g_i}^{-1}}$) to the corresponding group head $g_i$. Upon receiving this request message, group head $g_i$ decrypts $\{\mathrm{id}\}_{K_{g_i}^{-1}}$ with its public key ($K_{g_i}$). Once router id is valid, then $g_i$ sends a signed message ($\{M\}_{K_{g_i}^{-1}}$) along with a session key ($S_{K_{i,j}}$), where message $M$ consists of id and router timeout interval ($T_{i,j}$), maximum waiting time ($T_{i,j}^{\max}$) for the reply message.

Once, the new mesh router ($r_{i,j}$) receives the parameters from $g_i$, then $r_{i,j}$ has to join in backbone mesh within timeout interval ($T_{i,j}$). A router $r_{i,j}$ generates its own public and private key pair < ($K_{r_{i,j}}$), ($K_{r_{i,j}}^{-1}$) > and creates an authentication request ($\mathrm{ARQ}_{i,j}$) message to join in the backbone. AR $\mathrm{Q}_{i,j}$ message comprises $\{\{M\}_{K_{g_i}^{-1}}, \mathrm{id}, T_{i,j}, K_{r_{i,j}}, H(M')_{S_{K_{i,j}}}\}$, where $H(M')_{S_{K_{i,j}}}$ is a 512-bit unique code generated by SHA-512 Hash algorithm. The one-way hash function is calculated as $H(M')_{S_{K_{i,j}}} = \{\{M\}_{K_{g_i}^{-1}}, \mathrm{id}, T_{i,j}, K_{r_{i,j}}, S_{K_{i,j}}\} S_{K_{i,j}}$. Finally, a router $r_{i,j}$ disseminates $\mathrm{ARQ}_{i,j}$ request message at time $T$, and $r_{i,j}$ stores it as a time stamp ($T_s$). Once $\mathrm{ARQ}_{i,j}$ requeset is received by all its neighboring mesh router ($rn_{i,j}$), $rn_{i,j}$ decrypts the message $\{M\}_{K_{g_i}^{-1}}$ with the group head public key ($K_{g_i}$). A neighboring router $rn_{i,j}$ successfully verified router id and $T_{i,j}$, and if it is new router id, then $rn_{i,j}$ stores router id. After $rn_{i,j}$ rebroadcasts the $\mathrm{ARQ}_{i,j}$ message, dupilcate $\mathrm{ARQ}_{i,j}$ messages are dropped by veryfying the router id. This process continues until $\mathrm{ARQ}_{i,j}$ reaches to group head $g_i$.

On the other hand, $\mathrm{ARQ}_{i,j}$ message is received by another group's neighbor router $rn_{kl}$. This router can verify $\mathrm{ARQ}_{i,j}$ message because routers maintain public keys of trusted group heads (gateway nodes). Thus, $rn_{kl}$ decrypts the message $\{M\}_{K_{g_i}^{-1}}$ through the public key of the corresponding group head ($g_i$) and verifies router id and $T_{i,j}$. Once router id is not added in the table and if found that the $T_{i,j}$ is valid, the $r_{kl}$ stored the new router id in the authentication table. Further, the authentication message is transmitted to its group head $g_k$ through the path that was formed earlier. Once the authentication request message is received, other group head $g_k$ verifies the $\mathrm{ARQ}_{i,j}$ for its validity, and then, the message is unicasted to the associated group head $g_i$.

Once group head $g_i$ receives the $\mathrm{ARQ}_{i,j}$ message, $g_i$ verifies the received request message by its public key ($K_{g_i}$) and their session key ($S_{K_{i,j}}$). Once the message is found to be a valid, the group head $g_i$ stores $r_{i,j}$ public key ($K_{r_{i,j}}$) in authentication table with an authentication reply ($\mathrm{ARP}_{i,j}$) message (id, $T_{i,j}$, and $r_{i,j}$ public key $K_{r_{i,j}}$, ($\mathrm{ARP}_{i,j} = \{\mathrm{id}, T_{i,j}, \{K_{r_{i,j}}\}\}$). Consequently, $g_i$ signs on the authentication reply ($\mathrm{ARP}_{i,j}\mathrm{A}$) message with its private key ($K_{g_i}^{-1}$) and sends signed $\mathrm{ARP}_{i,j}$ message. After a neighboring router ($rn_{i,j}$) receives signed $\mathrm{ARP}_{i,j}$ message, $rn_{i,j}$ decrypts signed $\mathrm{ARP}_{i,j}$ message with public key ($K_{g_i}$). Once new router $r_{i,j}$ public key ($K_{r_{ij}}$) is verified, $rn_{i,j}$ adds the $K_{r_{i,j}}$ in their authentication table. Consequently, $rn_{i,j}$ forwards signed $\mathrm{ARP}_{i,j}$ message to next the immediate mesh router and repeats $\mathrm{ARP}_{i,j}$ message until signed $\mathrm{ARP}_{i,j}$ message reaches $r_{i,j}$.

A new mesh router ($r_{i,j}$) is successfully joined in backbone mesh once $r_{i,j}$ receives the signed $\mathrm{ARP}_{i,j}$ message in $T_s + T_i^{\max}$ the time interval; otherwise, $r_{i,j}$ rebroadcasts the $\mathrm{ARQ}_{i,j}$ message once timeout interval $T_{i,j}$ is not expired. In this sequance, $g_i$ disseminates router id and $K_{r_{i,j}}$ to other group heads for updating their authentication tables $\mathrm{AT}_{i,j}$ and $\mathrm{AT}_t$.

The valid mesh routers use their key pairs for the secure communication. Mesh router ($r_{i,j}$) authentication request and response message reachability are explained in Algorithms 1 and 2.

Figure 2 summarizes the crucial technical flow of Algorithm 1. According to the aspects, the algorithm validates mesh router attributes and makes the valid routers authentic entities in the network. In this connection, each router raises an authentication request message from inside the network and through the gateways. The authentication request messages are validated using router identifiers and network attributes initially to find the valid requests. On the basis of valid identifiers, the request has been forwarded into the network. In the next level, the requesting router characteristics are authenticated based on mesh configuration properties and gateway attributes.

On the successful validation, the authentication requests are forwarded to the neighbor nodes for ensuring local authentication policies at each node. Accordingly, the network path is protected from attacks.

Figure 3 illustrates the functions of Algorithm 2. Algorithm 2 describes the authentication procedures in order to identify the fake reply attacks. In this regard, Figure 3 shows the mesh node's reply validation and isolation tasks based on their correctness. In the first level, Figure 3 gives the validation of network path and destination causes in the replies.

The valid reply is forwarded to neighbor nodes for validating Address Resolution Protocol (ARP) messages, routing node's public keys, identities, time stamps, and other

/* Initial mesh router id validation*/
//intput: Gateway nodes(G<-{$g_1$,$g_2$,$g_3$,$g_4$,……$g_n$},
//Routers(R<-{{ $r_{1,1}$,$r_{1,2}$ ⋯ ..$r_{1,n}$ }, { $r_{2,1}$,$r_{2,2}$ ⋯ ..$r_{2,n}$ },……{ $r_{n,1}$,$r_{n,2}$ ⋯ ..$r_{n,n}$ }),),
//Authentication Request Message ARQ= $\{M, id, T, K_r, H(M)\}$
//Authentication Tables and router and gateway nodes public and private key pairs
flag=0 //Invalid or fake request packet
Mesh router ($r_{i,j}$) sends a request ($\{id\}_{K_{g_i}^{-1}}$) to $g_i$
$g_i$ decrypts $\{id\}_{K_{g_i}^{-1}}$ with its public key ($K_{g_i}$ )
if ($\{id\}_{K_{g_i^{-1}*K_{g_i}}}$ = Successful &router id∈$AT_i$ )
$g_i$ sends a signed message ($\{M\}_{K_{g_i}^{-1}}$) to $r_{i,j}$ where $M$ ={ $id$, $T_{i,j}$,$T_i^{\max}$ }, $S_{K_{i,j}}$.
else
  $g_i$ does not send a reply message to $r_{i,j}$
    /* Deploying $r_{i,j}$ in the backbone mesh*/
      $r_{i,j}$ generates its own public and private key pair ($K_{r_{i,j}}$, $K_{r_{i,j}}^{-1}$)
        $r_{i,j}$ broadcasts a $ARQ_{i,j}$={$\{M\}K_{g_i}^{-1}$, $id$, $T_{i,j}$, $K_{r_{i,j}}$, $H(M')_{S_{K_{i,j}}}$ } and sets $T_s$=$T_c$
                    // $T_c$ is packet send/receive time
$ARQ_{i,j}$ received by $rn_{k,l}|g_t$ ; $rn_{k,l}|g_t$ extract $M = \{M\}_{K_{g_i}^{-1}*K_{g_i}}$ from the $ARQ_{i,j}$ using $K_{g_i}$
if ( $\{M\}_{K_{g_i}^{-1}*K_{g_i}}$ = Successful )
  if (k=i) //neighboring router $rn_{k,l}$∈$g_i$
    if ( $T_{i,j} > T_c$ & router id ∉ $AT_{k,l}$)
      flag=1
        $rn_{k,l}$ stores router id & rebroadcasts $ARQ_{i,j}$
  **else** if ( $k \neq i$) //neighboring router $rn_{kl}$∈$g_i$
      if ( $T_{i,j} > T_c$ & router id ∉ $AT_{k,l}$)
        flag =1
          $rn_{k,l}$ stores router id & forwards $ARQ_{i,j}$ to $g_k$
    **else** if ( $t \neq i$ )//neighboring gateway $g_t \neq g_i$
          if ( $T_{i,j} > T_c$)
            flag =1
            $g_t$ forwards $ARQ_{i,j}$ to $g_i$
    **else** if ($t = i$) // neighboring gateway $g_t = g_i$
      if ( $T_{i,j} >= T_c$ & router id ∈ $AT_{i,j}$)
            $g_i$ creates $H(M'')_{S_{K_{i,j}}}$ using received $ARQ_{ij}$
          if ( $H(M')_{S_{K_{i,j}}}$=$H(M'')_{S_{K_{i,j}}}$)
          flag =1 // initial flag value set to zero
        $g_i$ stores the public key and drops $S_{K_{i,j}}$
          $g_i$ creates a signed $ARP_{i,j}(\{id, \{K_{r_{i,j}}\}\}_{K_{g_i}^{-1}})$
          Forwards signed $ARP_{i,j}$ to $r_{ij}$ through disjoint paths ($t_d$)
$g_i$ disseminates router id and $K_{r_{i,j}}$ to gateway nodes and its group members for updating their $AT_{i,j}$&$AT_t$
      else
          $g_i$ drops $ARQ_{ij}$ without reply message
    if(flag=0)
          $rn_{k,l}|g_t$ does not forward the $ARQ_{ij}$

Algorithm 1: Mesh router ($r_{ij}$) authentication request message reachability.

mesh attributes. Similarly, the node's (router) logical association is validated to confirm the authentication reply of the mesh router (node).

In the process of a router ($r_{i,j}$) deauthentication, $r_{i,j}$ creates a deauthentication request ($\text{DARQ}_{i,j}$) with its unique id. Consequently, $r_{i,j}$ signs on $\text{DARQ}_{i,j}$ message with its private key ($K_{r_{i,j}}^{-1}$) and forwards $\{\text{DARQ}_{i,j}\}_{K_{r_{i,j}}^{-1}}$ message to its group head $g_i$ through "$t_d$" number of node disjoint paths in backbone at time $T$. Once signed, $\text{DARQ}_{i,j}$ message is received by a neighboring router/gateway ($rn_{i,j}/g_t$); it decrypts this message by the mesh router's public key ($K_{r_{i,j}}$).

Once signed $\text{DARQ}_{i,j}$ message is valid, then $rn_{i,j}/g_t$ transmits this message to the subsequent routers. Otherwise, $\{\text{DARQ}_{i,j}\}_{K_{r_{i,j}}^{-1}}$ message is dropped by $rn_{i,j}$. Upon receiving

*Intput: Gateway nodes(G<-{$g_1$,$g_2$,$g_3$,$g_4$.....$g_n$},*
*Routers(R<-{{ $r_{1,1}$,$r_{1,2}$ ⋯ ..$r_{1,n}$ }, { $r_{2,1}$,$r_{2,2}$ ⋯ ..$r_{2,n}$ },.....{ $r_{n,1}$,$r_{n,2}$ ⋯ ..$r_{n,n}$ }),),*
*Authentication Request Message ARP=$\{id, T, K_r\}$*
Authentication Tables and router and gateway nodes public and private key pairs
*flag=0 //invalid or fake reply messages*
*$rn_{k,l}|g_t|g_i$ receives $\{ARP_{i,j}\}K_{g_i}^{-1}$*
*if $(rn_{k,l}/g_t \neq r_{i,j}\&g_i)$*
*$rn_{k,l}$ / $g_t$ in $t_d$ paths verifies $\{ARP_{i,j}\}_{K_{g_i}^{-1}}$ with $K_{g_i}$ //intermediate nodes*
*if $(\{ARP_i\}K_{g_i}^{-1} * K_{g_i} = Successful)$*
*flag=1*
*$rn_{k,l}$ / $g_t$ add new router { router id′, $k_{i,j}$ } in the $AT_{k,l}/AT_t$*
*$rn_{k,l}$ / $g_t$ forwards signed $ARP_{i,j}$ to the next router*
*else if( $rn_{k,l}= r_{i,j}$ )*
*$r_{i,j}$ verifies $\{ARP_{i,j}\}_{K_{g_i}^{-1}}$ with $K_{g_i}$ //destination node*
*if( $\{ARP_i\}_{K_{g_i}^{-1}*K_{g_i}}$ = successful )*
*if( $\{ARP_{i,j}\}_{K_{r_{i,j}}^{-1}}$ arrival time at $r_{i,j} \leq T_s + T_i^{\max}$)*
*flag=1*
*$r_{i,j}$ is successfully joined in backbone mesh*
*else if $(T_c < T_{i,j})$*
*flag=1*
*$r_{i,j}$ sends new $ARQ_{i,j}$ in backbone mesh*
*mesh routers drop { $r_{i,j}$, id } from their corresponding authentication table*
*if(flag=0) //intermediate nodes and destination node*
*$rn_{k,l}|g_t$dorps $\{ARP_{i,j}\}_{K_{g_i}^{-1}}$ with no response*

Algorithm 2: Mesh router ($r_{ij}$) authentication replay message reachability.

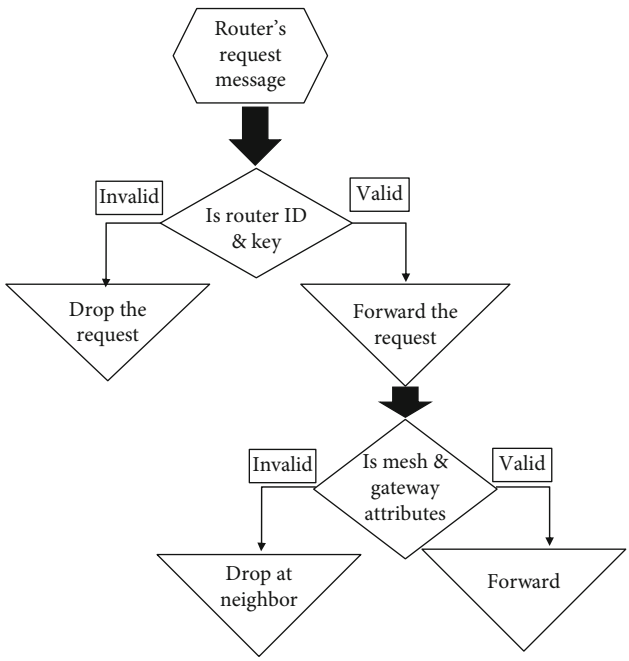



Figure 2: Mesh router ($r_{ij}$) authentication request message reachability.

the $\{\text{DARQ}_{i,j}\}_{K_{r_{i,j}}^{-1}}$ message, the group head $g_i$ verifies this message by $r_{i,j}$ public key. If the message is legal, then $g_i$ deletes the router {id, $K_{r_{il}}$} from authentication table ($\text{AT}_i$). Later, the group head $g_i$ creates a signed deauthentication reply ($\text{DARP}_{i,j} = \{\text{id}, k_{r_{i,j}}\}_{K_{g_i}^{-1}}$) message, and it forwards signed $\text{DARP}_{i,j}$ to router $r_{ij}$ through disjoint paths ($t_d$); also, the $r_{i,j}$ deauthentication information disseminates to other group heads and its group members [27–29].

Figures 4 and 5 depict the details of deauthentication procedures as discussed. These figures are representing Algorithms 3 and 4, respectively.

Figure 4 has analyzed the router's or node's authentication request and its successful completion upon various validation procedures. Consequently, the request is involved in deauthentication procedures and signature validation procedures in each router (gateway or mesh node). A gateway router or any internal mesh router is responsible for extracting the path attributes, channel participant attributes and digital signatures of each initiative. According to that, the internal mesh node or gateway traffics are identified for deauthentication policies as shown in Algorithm 3 and Figure 4.

In the same way, Figure 5 shows the deauthentication steps on response messages and validation steps on disjoint paths in the network. As mentioned in Figure 5 and Algorithm 4, the false responses and false logical paths are

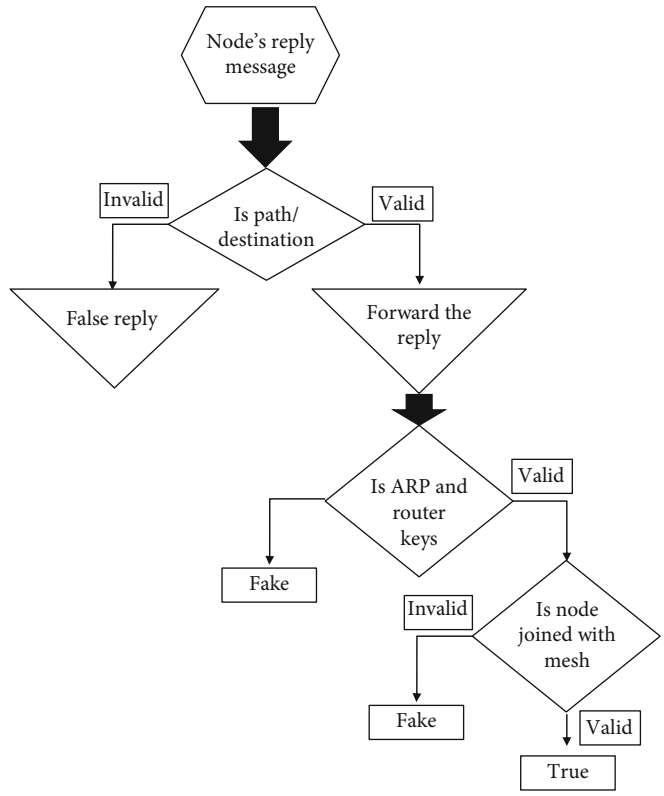



Figure 3: Mesh router ($r_{ij}$) authentication reply message reachability.

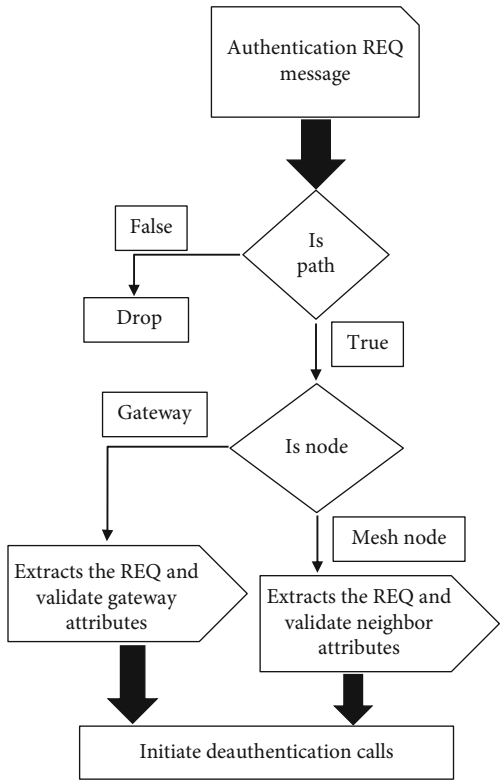



Figure 4: Mesh router ($r_{ij}$) deauthentication request message reachability.

identified using signature verification policies and identity extraction. The technical details are given in Algorithm 4.

Once a neighboring mesh router/gateway ($rn_{i,j}/g_t$) receives signed $\text{DARP}_{i,j}$ message, router/gateway $rn_{i,j}/g_t$ decrypts signed $\text{DARP}_{i,j}$ message using group head's public key ($K_{g_i}$). Once group head $g_i$ public key ($K_{g_i}$) is successfully decrypts the signed $\text{DARP}_{i,j}$ message, then $rn_{i,j}/g_i$ deletes the router {id, $K_{r_{il}}$} from the authentication table ($\text{AT}_{i,j}/\text{AT}_t$) and forwards signed $\text{ARP}_{i,j}$ message to the subsequent routers and gateways, and this process repeats until signed $\text{DARP}_{i,j}$ message reaches to $r_{i,j}$. Once the signed $\text{DARP}_{i,j}$ message is received, $r_{i,j}$ is completely isolated from the backbone network [30–32]. Mesh router ($r_{i,j}$) deauthentication is explained in algorithms 3 and 4.

*3.4. Security Analysis.* In this section, we analyze the security of the proposed distributed authentication technique against various authentication attacks like impersonation attacks, replay attacks, deprivation attacks, and information security distributed denial of service attacks. Various inferences show that the secure multiwatchdog system could guard nodes that have maximum coverage. Additionally, single point failure of a single watchdog system shall be avoided through the deployment of the secure multiple watchdog system.

The impersonation attack harms the router once a router node broadcasts an authentication request message. However, other fake gateway nodes respond to the router request message. In the proposed approach, any node replies to the

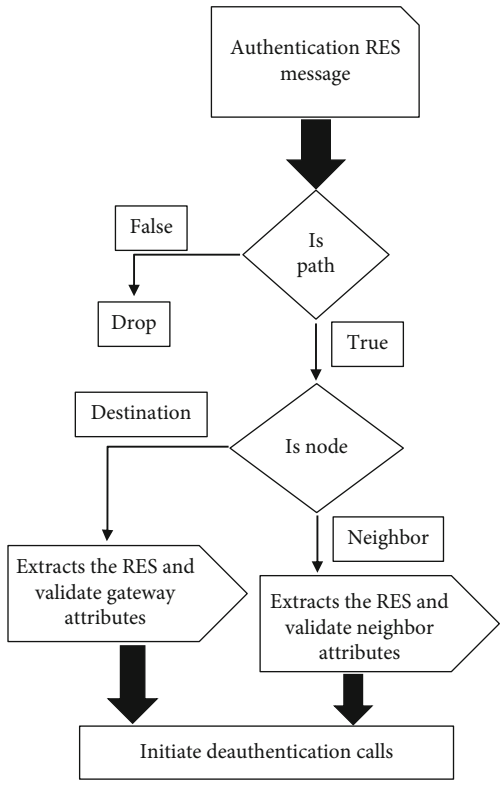



FIGURE 5: Mesh router ($r_{ij}$) deauthentication response message reachability.

router other than the corresponding gateway node. It can be easily detected by the router by verifying the signature on the reply message with the public key of the corresponding group head. Replay attack creates a serious problem in WMN. The authentication request message sent out by the legitimate mesh router can be intercepted and replayed by an attacker in order to join the mesh network. Once the attack is successfully initiated, the attacker enters the active phase and sends messages on behalf of the target node. In our proposed approach, each request message is protected from the replay attack, by maintaining the sequence number and time stamp of the request message. In this case, the attacker employs a replay attack in the mesh node, which is easily detectable and dropped. The node deprivation attack is similar to the replay attack in that it starts with the capture of the legitimate mesh router's deauthentication request message. After that, an attacker replays the deauthentication request message in order to isolate the mesh router when it rejoins the network [33–35].

The authentication flooding attack is raised to restrict the transmitting messages for every $t$ seconds. Once the $t$ value lies between 10 seconds and 100 seconds, we can prevent the DoS and DDoS attacks. DDoS attackers work together to flood the fake authentication request messages to isolate the target mesh router during a colluding attack. A consequence of this is that the authentication request message from the mesh router is not received by the gateway node. The proposed mechanism resists DDoS attack paths between the mesh router and the gateway node up to "$t_d - 1$" where "$t_d$" is the total number of node disjoint paths.

*3.4.1. Attack Model Definition.* Assume that the attacker AT_$N$ initiates authentication attacks such as false identification, identity duplication, data repetition, identity masking, and other malicious activities around the set of network nodes, $S(n)$. In this model, the attacker AT_$N$ has the attack properties, $A(P) = \{i, j, k, l\}$ as predefined attack rules to harm the network.

The properties $i, j, k, l$ denote the attack engines. In the overall mesh network, there are $n *$ AT_$N$ attackers can raise $n * A(P)$ possibilities of authentication attacks as mentioned earlier. The $n *$ AT_$N$ attackers can be either external participants or compromised nodes in the network. In this regard, crucial authentication attacks need to be identified through different security analysis models. As mentioned earlier, router-centric authentication and deauthentication procedures analyze the outcomes as given below.

*3.4.2. Lemma and Proof.* The development of proposed security analysis model, $P(\text{Auth})$ against $n * A(P)$ of attackers $n *$ AT_$N$ creates a stable legitimate property group $G(l)$ in the network. The $G(l)$ over the security perimeter $S(p)$ called as stable security group $SG(l)$. In addition, this group allows the network system to choose a security bias parameter, $\varnothing \longrightarrow \{0, 1\}$ with dual-collision points between both sender and receiver. The security analysis steps and proofs are as follows:

(i) Call Algorithms 1 and 2 at each router against $n * A(P)$

(ii) Set timestamp, $T\_$ at both ends, $T_$Sender and $T_$Receiver

(iii) Data construct, $n_{\text{data}} = m \| T\_$

(iv) Construct router authentication tuple, $T_$Auth

(v) Send $n_{\text{data}} \| T_$Auth, as $A(u).dt$

(vi) Receive $n_{\text{data}} \| T_$Auth at receiver

(vii) Call Algorithms 2.1 and 2.2 at each router against $n * A(P)$

(viii) Do deauthentication and extract the original data

It has to be proved as $A(u).dt$ has the consistency range $\varnothing \longrightarrow \{0{,}0.5\}$ at changing time interval $dt$. Assume that $n * A(P)$ has hold the permutations on $\{i, j, k, l\}$ as $\{p, q, r, s\}$ to initiate the attacks in to the nodes or channels. This lemma needs to prove that a quadruple of $\{p, q, r, s\}.dt \leq l(A(u).dt \| D(u).dt)$. In this proof, $l(A(u).dt \| D(u).dt)$ indicates the expected legitimate properties of derived authentication and deauthentication policies. This is common security need for $l(A(u).dt \| D(u).dt)$ of mesh router's reachability and reply procedures. Under this case, $T_$Sender and $T_$Receiver are concatenated with original messages to counter measures against reply attack and flooding attack. The entire data

*Intput: Gateway nodes(G<-{$g_1$,$g_2$,$g_3$,$g_4$…….$g_n$},*
*Routers(R<-{{ $r_{1,1}$,$r_{1,2}$ ⋯ ..$r_{1,n}$ }, { $r_{2,1}$,$r_{2,2}$ ⋯ ..$r_{2,n}$ },……{ $r_{n,1}$,$r_{n,2}$ ⋯ ..$r_{n,n}$ }),),*
*Authentication Request Message DARQ={id.$K_r$}*
Authentication Tables and router and gateway nodes public and private key pairs
*flag=0 //invalid or fake request message*
*$r_{i,j}$ sends a signed deauthentication reply ($\{DARQ_{i,j}\}_{K^{-1}_{r_{i,j}}}$ ) message to $g_i$ through node disjoint paths ( ' $t_d$ ') and sets $T_s$ value*
*$\{DARQ_{i,j}\}_{K^{-1}_{r_{i,j}}}$ message received by any of its neighboring node/nodes ($rn_{k,l}$ / $g_t$ )*
*$rn_{k,l}$ / $g_t$ verifies $\{DARQ_{i,j}\}_{K^{-1}_{r_{i,j}}}$ with $K_{r_{i,j}}$*
*if( $\{DARQ_{i,j}\}_{K^{-1}_{r_{i,j}} * K_{r_{i,j}}}$ =Successful)*
*Neighboring node ($rn_{k,l}$ / $g_t$) extracts router id from $\{DARQ_{i,j}\}_{K^{-1}_{r_{i,j}} * K_{r_{i,j}}}$*
*if( $\{router\,id', k_{r_{i,j}}\} \in AT_{k,l}/AT_t$) //gateway id $t \neq i$*
*flag =1*
*$rn_{k,l}$ / $g_t$ forwards $\{DARQ_{i,j}\}_{K^{-1}_{r_{i,j}} * K_{r_{i,j}}}$ to $g_i$ through known path*
*else if( $\{\text{router id}', \text{k}_{\text{r}_{\text{i,j}}}\} \in AT_i$) //gateway id $t = i$*
*flag =1*
*$g_i$ deletes $\{router\,id', k_{r_{i,j}}\}$ information in the $AT_i$*
*$g_i$ creates a signed $DARP_{i,j}$ ( $\{id, k_{r_{i,j}}\}_{K^{-1}_{g_i}}$)*
*$g_i$ forwards signed $DARP_{i,j}$ to $r_{ij}$ through disjoint paths ($t_d$)*
*$g_i$ disseminates the deleted $\{router\,id', k_{r_{i,j}}\}$ to all gateways*
*if (flag =0)*
*$rn_{k,l}$ / $g_t$ drops $\{DARQ_{i,j}\}_{K^{-1}_{r_{i,j}}}$ without any response*

Algorithm 3: Mesh router ($r_{ij}$) deauthentication request message reachability.

Intput: Gateway nodes(G<-{$g_1$,$g_2$,$g_3$,$g_4$…….$g_n$},
*Routers(R<-{{ $r_{1,1}$,$r_{1,2}$ ⋯ ..$r_{1,n}$ }, { $r_{2,1}$,$r_{2,2}$ ⋯ ..$r_{2,n}$ },……{ $r_{n,1}$,$r_{n,2}$ ⋯ ..$r_{n,n}$ }),),*
*Authentication Request Message DARP={id.*Kr}
Authentication Tables and router and gateway nodes public and private key pairs
*flag=0 //invalid or fake request message*
*$\{DARP_{i,j}\}_{K^{-1}_{g_i}}$ received by intermediate nodes ($rn_{k,l}$ / $g_t$) or destination node( $r_{i,j}$ )*
*if( $rn_{k,l}$ / $g_t \neq \text{r}_{i,j}$ / $g_i$ )*
*$rn_{k,l}$ / $g_t$ in $t_d$ paths verify $\{DARP_{i,j}\}_{K^{-1}_{g_i}}$ with $K_{g_i}$ //intermediate nodes*
*if ($\{DARP_{i,j}\}_{K^{-1}_{g_i} * K_{g_i}}$ = Successful)*
*flag =1*
*$rn_{k,l}$ / $g_t$ deletes { $router\,id', k_{i,j}$ } in the $AT_{k,l}/AT_t$*
*$rn_{k,l}$ / $g_t$ forwards signed $DARP_{i,j}$ to the next router*
*else if( $rn_{k,l} = r_{i,j}$ )*
*$r_{i,j}$ verifies $\{DARP_{i,j}\}_{K^{-1}_{g_i}}$ with $K_{g_i}$ //destination node*
*if( $\{DARP_{i,j}\}_{K^{-1}_{g_i} * K_{g_i}}$ = successful )*
*if( $\{DARP_{i,j}\}_{K^{-1}_{r_{i,j}}}$ arrival time at $r_{i,j} \leq T_s + T_i^{\max}$)*
*flag =1*
*$r_{i,j}$ is isolated from the backbone mesh*
*else*
*$r_{i,j}$ creates and sends a new $\{DARQ_{i,j}\}_{K^{-1}_{r_{i,j}}}$ message to $g_i$*
*through node disjoint paths( $t_d$*

Algorithm 4: Mesh router ($r_{ij}$) deauthentication response message reachability.

communication sessions are authenticated at each router points to secure the network.

*3.5. Router Message Reachability Analysis.* Attackers are using DDoS attacks to disturb the functions of WMNs. Since these attackers are preventing genuine mesh router connection activities, they are having an impact on the network's scalability. Once a centralized system authenticates and deauthenticates backbone mesh routers, the routers are at risk of being compromised. Mesh routers' cooperative behavior reduces the impact of collaborating attackers on the backbone mesh. For heterogeneous and homogeneous radio-range wireless devices, Bhoi et al. [36] proposed a network node connection probability model based on probability distributions. In this model, node communication ranges and overall network size are linked impactfully with coverage factors [37].

The reachability of communications in a hostile network has required certain changes to this concept. The connectivity probability model is used for analyzing the DAPM in comparison with other current centralized authentication schemes such as Mobisec and DSA-Mesh. In this scenario, the percentage of malicious mesh routers varies from 0% to 100% causing a hostile backbone mesh to be created. We specify the notations that are used in this model as follows:

(1) The number of gateways in the WMN is $N_G = |G|$

(2) The number of mesh routers in the WMN is $N_R = |R|$

(3) The number of gateway nodes receives the authenticate request ($\mathrm{ARQ}_{i,j}$) from a mesh router ($r_{i,j}$) is $N_{G'} = |G'|$

(4) Total number of backbone nodes in the WMN is $N_{G+R} = |G| + |R|$

(5) Define the density $\rho = (\mathrm{Active\_Links}_G + \mathrm{Active\_Links}_R)/\mathrm{Possible\_Links}_G + \mathrm{Possible\_Links}_R$

(6) Each router coverage area is $\pi r_j^2$ where $j = 1, 2, \cdots, J$

(7) Neighborhood connectivity (degree of a router) is $d_{\min}^{(k)}$ where $k = 1, 2, \cdots, n$

(8) Number of malicious nodes have a different communication range

$N_M = \sum_{j=1}^{J} m_j$, where $m_j$ is the number of malicious nodes that have the same communication range. Based on network node communication range, $N$number of backbone nodes are classified into$J$different communication nodes such as$N_{G+R}$=$\sum_{j=1}^{J} n_j$, where $n_j = |G' + R'|$ subset of gateway and routers have equal communication range. The probability of a message is not reachable ($P_N(\mathrm{Auth}_{i,j})$), and reachable ($P(\mathrm{Auth}_{i,j})$) at $g_i$ is found to be a principal component that gets reflected due to the effect of colluding attackers ($N_M$). The details are illustrated in

$$P_N\left(\mathrm{Auth}_{i,j}\right) = \exp\left(-\sum_{m=1}^{J} d_{\min}^{(k)} * \rho * N_M * \pi r_{\min}^2\right), \quad (1)$$

where $k$ denotes minimal node degree and the "effective range" $r_{\min} = \min\{\{r_j\} j = 1, \cdots, |J|, r_{\min}\}$. Thus,

$$P\left(\mathrm{Auth}_{i,j}\right) = \left(1 - \left(P_N\left(\mathrm{Auth}_{i,j}\right)\right)\right)(N_R - N_M) * \frac{N_{G'}}{N_G}. \quad (2)$$

Equation (2) shows the length of the communication range between backbone nodes, the density of mesh routers, and the number of gateway nodes. These entities have an impact on the readability of messages from a mesh router to a gateway [38–40]. As per the proposed DAPM, the number of gateways required for routers differs significantly from the number of gateway nodes required by the existing techniques (Mobisec and DSA-Mesh). As a result, we compare the performance of proposed and existing solutions by changing the number of gateway nodes in each solution.

In Figures 6(c) and 6(d), we use $r_1 = 200$ m, $r_2 = 250$ m, and $d_{\min}^{(k)}$) =1 and 2 to compare the mesh router reachability of DAPM, Mobisec, DSA-Mesh, AHKM, and MENSA. Figures 6(a)–6(d) show the results of this comparison.

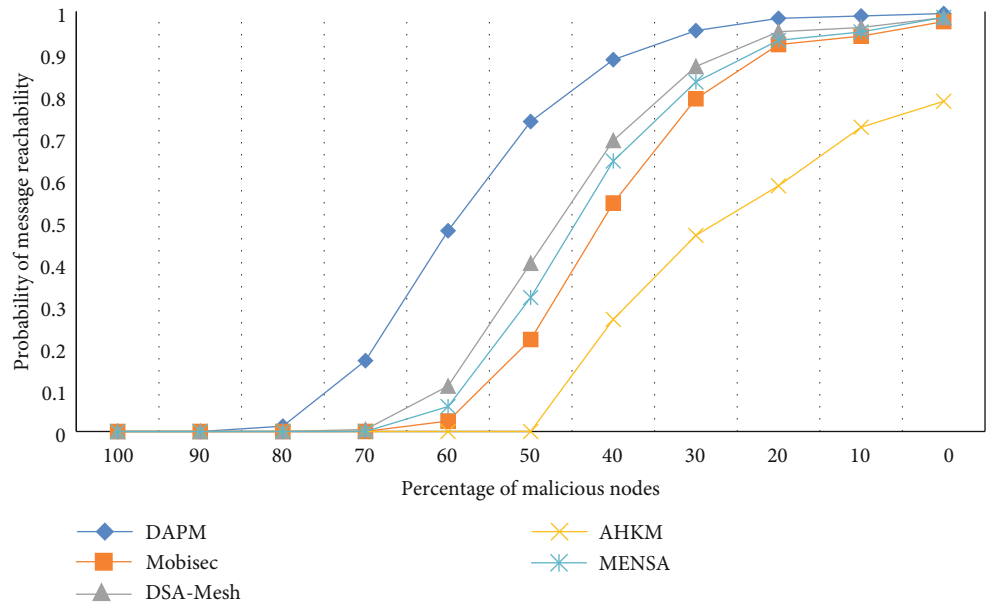
Figures 6 and 7 depict the probability of mesh router message reachabilities for the proposed DAPM, where the existing schemes are configured with the number of group head values of 5 and 10. Once comparing $N_G$ values of 5 and 10, the proposed system gives better performance for authentication and deauthentication policies [25–27]. In order to authenticate mesh router in DSA-Mesh, the mesh router message must be received by a minimum of ($N_G$/2) + 1 group heads.

On the other hand, AHKM only authenticates one-hop distance routers. The network radio range to join new routers to the network is limited, and MENSA nodes are directly connected to group heads. All network nodes should be adjacent to group heads to join or leave the network [41–44].

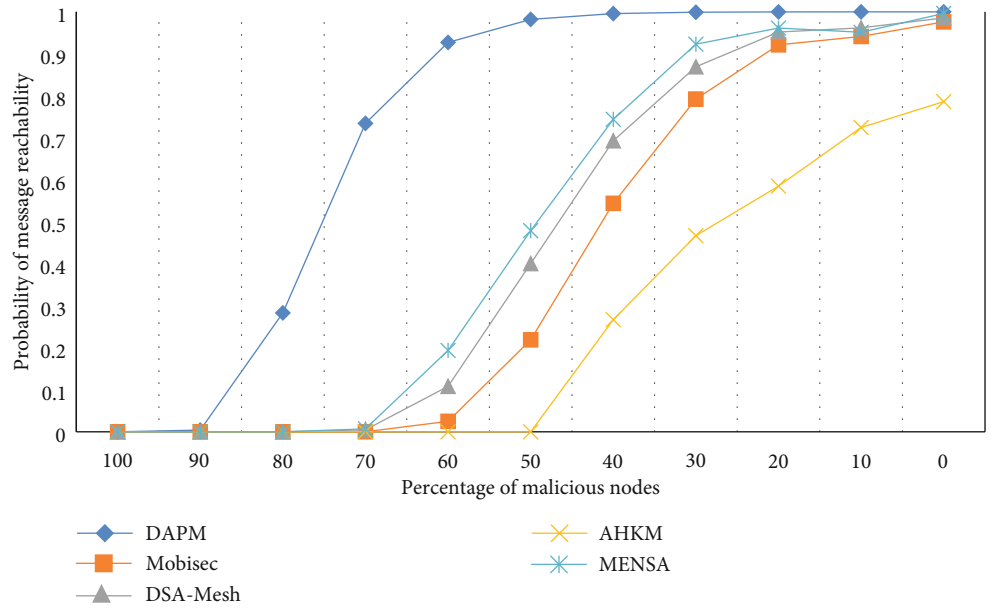
The proposed DAPM message reachability is very high due to the fact that the routing message process by any group head [45, 46].

According to Figure 6, the average message reachability of the DAPM is 69%, the existing scheme's average message reachability is 60%, MENSA average message reachability is 58%, Mobisec average message reachability is 57%, and AHKM average message reachability is 27% in the hostile network (0-100 percent malicious nodes), for an $N_G$ value of 5. It has been shown that the proposed DAPM is better than DSA-Mesh, MENSA, Mobisec, and AKHM by 9%, 10%, 12%, and 42%, respectively.

Based on the message reachability analysis with 10 group nodes, the average message reachability of the proposed DAPM is 76%. The existing scheme's average message reachability is 64%, MENSA's average message reachability is 62%, Mobisec's average message reachability is 59%, and AHKM's average message reachability is 35% in a hostile network, as shown in Figures 7(a)–7(d) (0–100% malicious




(a) $r_1 = 150$ m, $r_2 = 200$ m, and degree = 1




(b) $r_1 = 150$ m, $r_2 = 200$ m, and degree = 2

Figure 6: Continued.

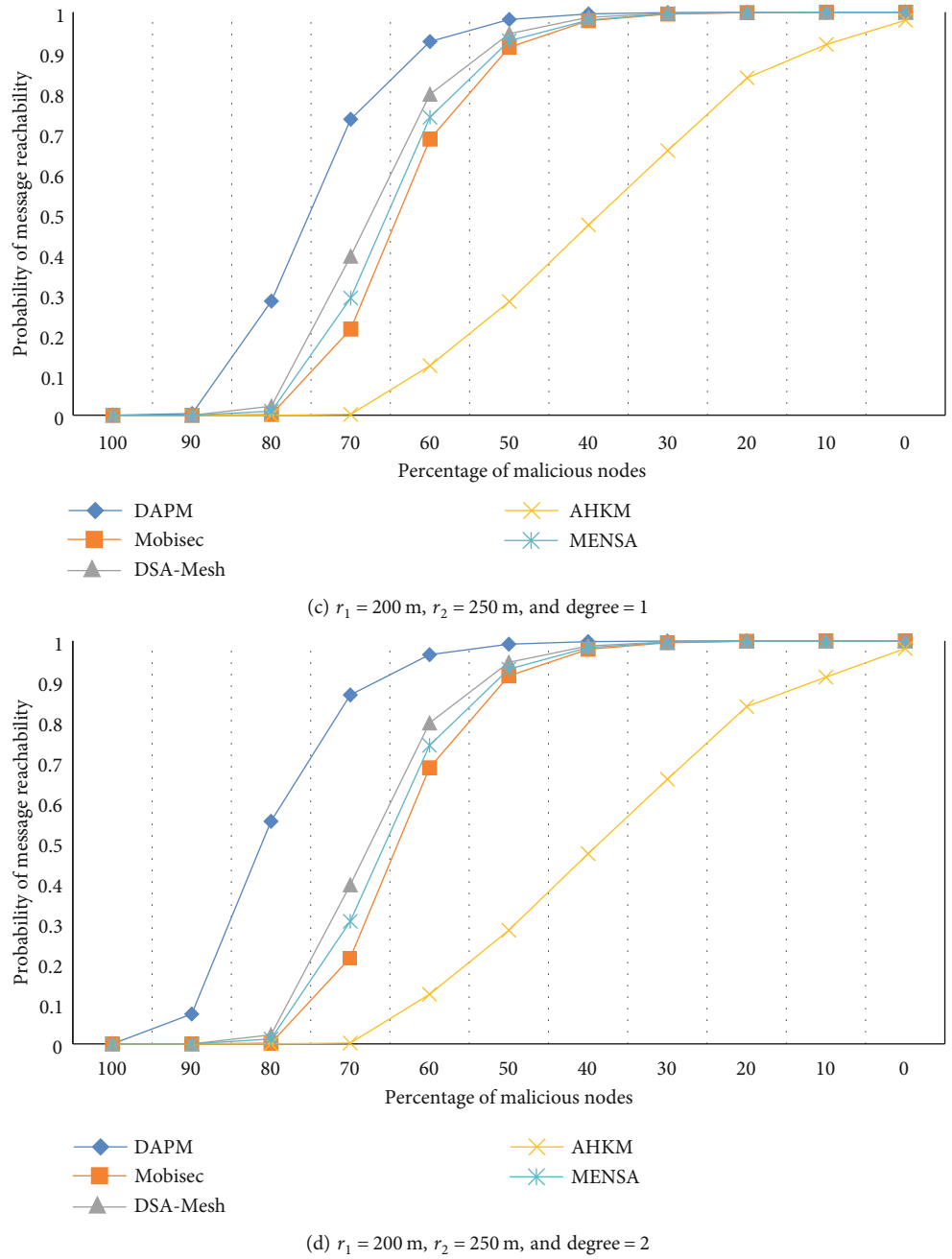



FIGURE 6: (a) Mesh router message reachability (degree = 1). (b) Mesh router message reachability with $N_G = 5$. (c) Mesh router message reachability. (d) Mesh router message reachability with $N_G = 5$.

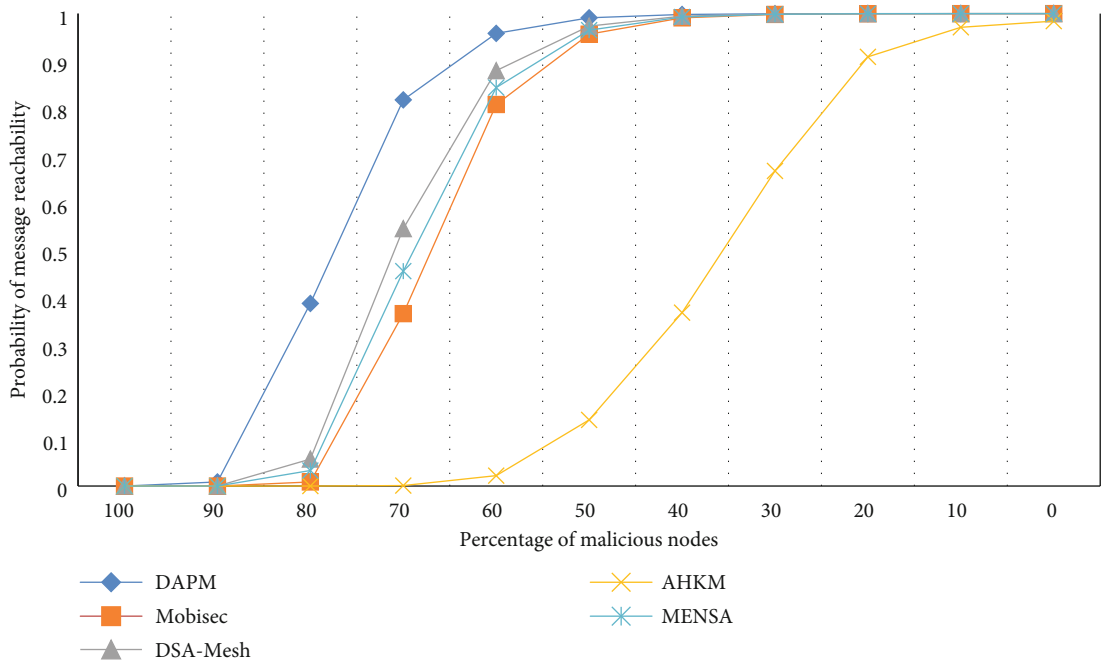
nodes). According to the authors, when $N_G$ is set to 10, the proposed DAPM-DA performs 12% better than DSA-Mesh, 14% better than MENSA, 17% better than Mobisec, and 31% better than AHKM.

DAPM reduces the severity of network attacks by increasing the range of transmission or the number of routers in the backbone mesh [47, 48]. Since the proposed DAPM is developed based on heterogeneous device connectivity probability model, it outperforms DSA-Mesh, MENSA, Mobisec, and AHKM in a hostile network [28–30]. In the next section, a simulation study has been performed to compare the proposed DAPM with the DSA-Mesh, MENSA, Mobisec, and AHKM schemes, with the $N_G$ value of each scheme being varied.

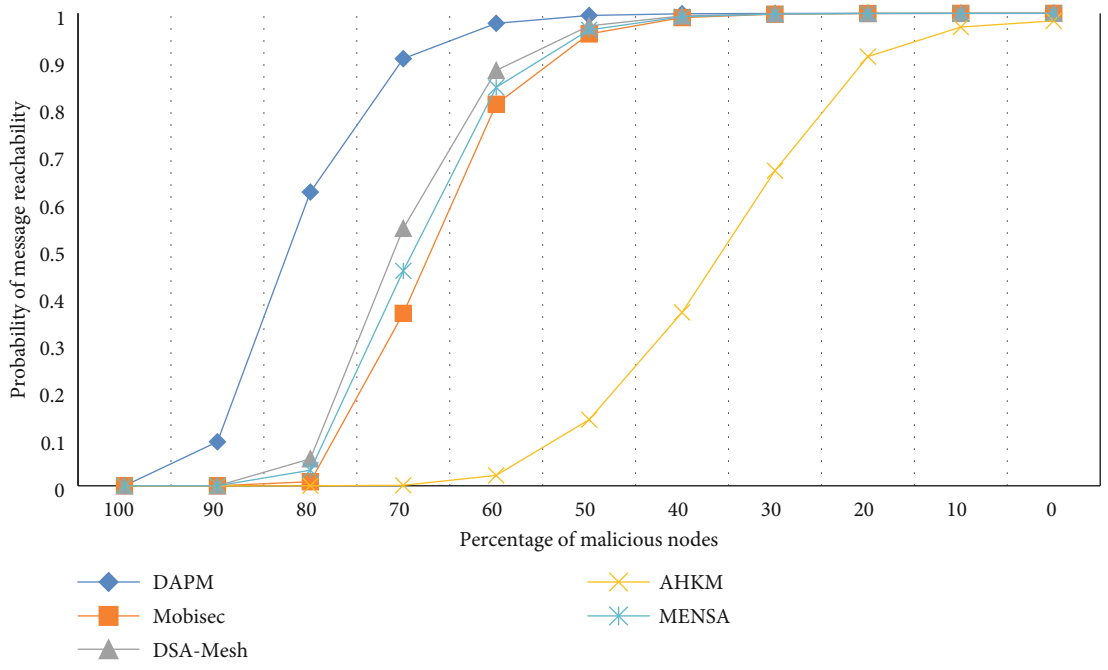
## 4. Simulation Results

In this work, network simulator (NS-2) is used to implement the proposed DAPM as well as existing schemes such as DSA-Mesh, MENSA, Mobisec, and AHKM.

A uniform random generator selects the $x$ and $y$ coordinates of $n_r$=100 mesh routers on a 1000 meter × 1000 meter

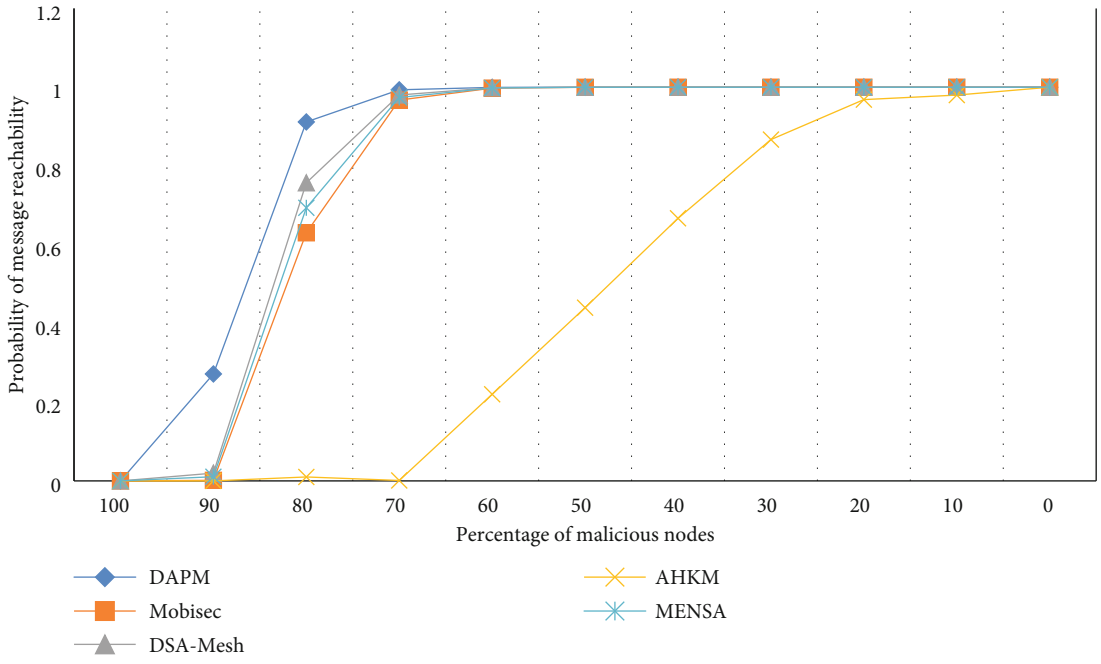



(a) $r_1 = 150$ m, $r_2 = 200$ m, and degree = 1

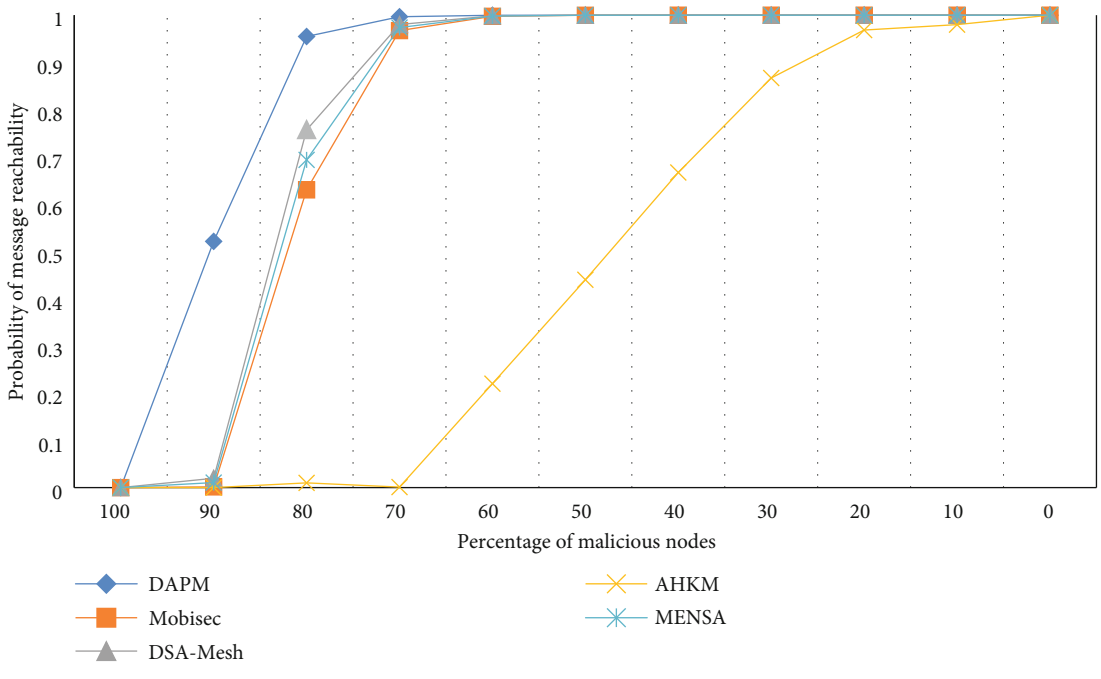



(b) $r_1 = 150$ m, $r_2 = 200$ m, and degree = 2

Figure 7: Continued.




(c) $r_1 = 200$ m, $r_2 = 250$ m, and degree = 1




(d) $r_1 = 200$ m, $r_2 = 250$ m, and degree = 2

Figure 7: Mesh router message reachability with $N_G = 10$.

(m) area in the simulation environment [49]. Particularly, the NS-2 tool has been used for creating the WMN circumstance with required nodes (0 to 100). Among these nodes, internal mesh nodes and gateway nodes communicate each other to transmit the data. In this case, the energy level of gateway nodes and internal nodes is configured as 50 joules and 30 joules, respectively. Similarly, each node has limited transmission range from 150 meter to 250 meter (omnidirectional). In addition, the implementation of proposed and existing techniques is done using object tool command language platform. The performance of the DAPM, DSA-Mesh, MENSA, Mobisec, and AHKM schemes is evaluated using various metrics. The legitimate mesh router messages are dropped by the malicious nodes in the network. The results are considered for an average of 1000 simulations, with each simulation lasting 100 seconds. Out of 100 mesh routers, 50 have a transmission range of 150 m, while the remaining mesh routers have a transmission range of 250 m.

In the network layer, we consider the 802.11 MAC layer protocol and the AOMDV path discovery protocol, and we

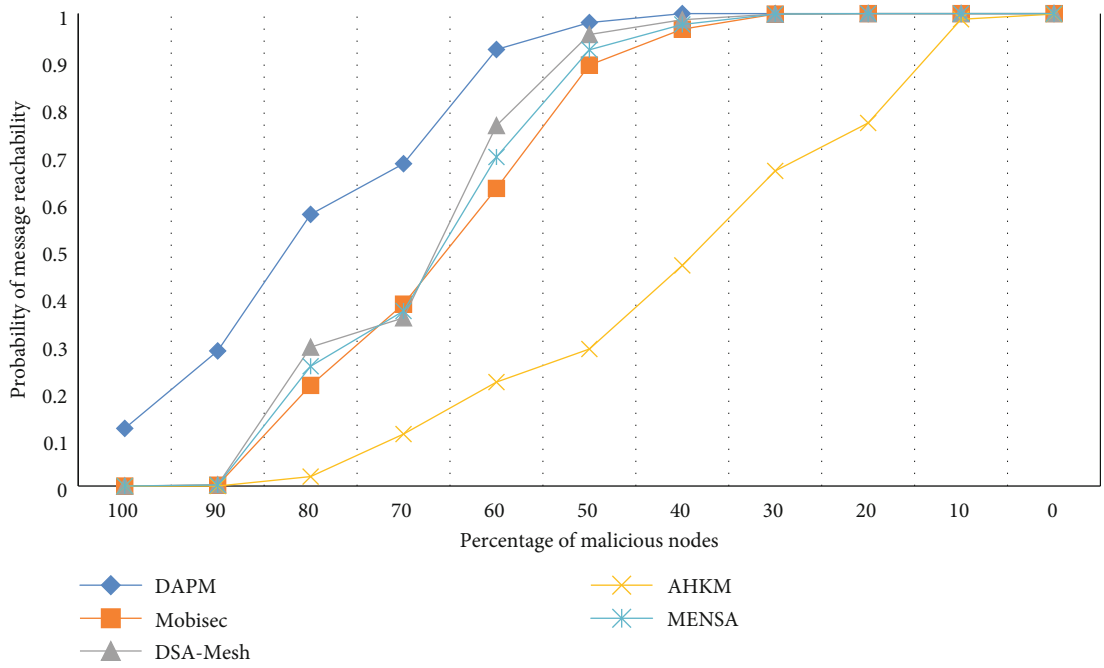



Figure 8: Message request reachability with $N_G = 5$.

generate 100 bytes of messages for mesh router authentication and deauthentication. To simulate the WMN, we set the pause time to 2 ms. We established communication ranges ranging from 150 meter to 250 meter for both long-distance and short-distance wireless links. We employ a random waypoint model for node mobility. We ran 10,000 simulations in this setup, varying the number of malicious nodes from 0 to 100%.

Compared to the proposed model, existing techniques provide notable security provisions. DSA-Mesh is the existing technique to enable distributed key management principles in each mesh router. In this regard, the Digital Signature Algorithm (DSA) is used to ensure distributed authenticated solutions. Compared to other existing techniques, DSA-Mesh is an effective authentication technique that is suitable for mesh networks and large distributed networks. Due to this reason, DSA-Mesh attains an optimal message reachability rate than other existing techniques.

On the scope, a two-level verification mechanism is used in AHKM, with a one-hop path for nodes inside the cluster and a multihop path for nodes outside the transmission range. In a one-hop route, all nodes have direct access to the base station, and nodes send authentication requests directly to the base station. In a multihop route, nodes cannot send messages directly to the base station; instead, they must send the message to a neighboring node, which can then pass it on to the base station. This approach typically employs a two-hop distance to authenticate a new node.

MENSA, the first hybrid key management and authentication solution in microgrids that includes public key infrastructure and web-of-trust concepts, was developed by Bolgouras et al. [33] MENSA's authoritative nodes issue the certificate to the other nodes in the network. Each node's certificate is checked by an authoritative node. In this topology, if a node joins the network, all network nodes are connected in a ring. A new node that receives multiple certificates from various certifying authorities has a good chance of succeeding. The authoritative nodes must be within one hop of each other for new nodes to join. However, MENSA and AHKM are providing moderate results than the DSA-Mesh technique. Due to unstable key production and effective internal authentication procedures, these techniques are limited to distributed security policies.

In this concern, Mobisec provides the security architecture with data confidentiality and authentication policies. Mobisec has been specially made for WMN security at medium access control layer functions. On this basis, this approach is called Mobimesh with second-layer encryption principles. On the basis of overall comparison, the existing DSA-Mesh performs better than other techniques in terms of distributed authentication rules. At the same time, DSA-Mesh is limited in terms of dual point authentication policies (gateway/internal). The experiment has been conducted, and the performance of security systems is evaluated using the metrics such as message reachability rate, attack detection accuracy, packet delivery ratio (PDR), false acceptance rate (FAR), and false positive rate (FPR), computational complexity, and attack detection time.

Message reachability rate is defined as the rate of probability between the number of messages reached by each neighbor or gateway node and the total messages transferred in the network. Attack detection accuracy can be determined as the total number of malicious events detected from a total number of attacks initiated in the network. FAR is the rate determined as the number of malicious events counted as legitimate events in the WMN. In the contrast, FPR is measured as the number of events counted as malicious when they are really legitimate in the network. In addition, the

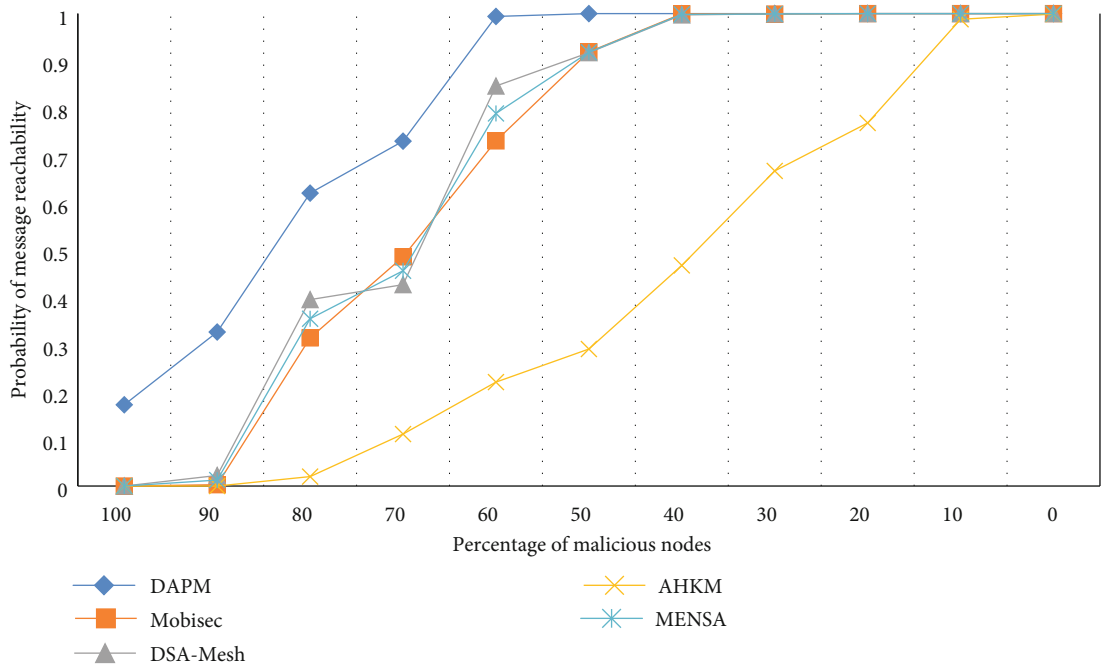



Figure 9: Message request reachability with $N_G = 10$.

Table 2: Performance analysis.

| Techniques | Average detection accuracy (%) | Average FAR (%) | Average FPR (%) | Average detection time (milliseconds) | Average PDR (%) | Overall computation complexity (milliseconds) |
|---|---|---|---|---|---|---|
| DAPM | 98.4 | 3.67 | 3.11 | 103.67 | 98.9 | 156.8 |
| DSA-Mesh | 90.6 | 10.98 | 11.34 | 145.67 | 91.3 | 193.4 |
| Mobisec | 88.6 | 13.78 | 14.11 | 189.24 | 83.5 | 237.1 |
| AHKM | 80.4 | 26.12 | 24.95 | 221.67 | 80.1 | 287.9 |
| MENSA | 85.7 | 14.34 | 15.18 | 199.55 | 81.4 | 255.6 |

overall time complexity taken by each algorithm is more important to understanding the timeline issues in the execution. On the other side, attack detection time helps to identify the time domain performance of each existing system and proposed DAPM. In this regard, time complexity and attack detection time are identified as the execution time taken by the algorithm phases and DDoS attack detection procedures, respectively. The experiment base measures the time complexity in terms of milliseconds.

Figure 8 depicts the performance of the DSA-Mesh, MENSA, Mobisec, and AHKM schemes when $N_G$ is set to 5. DAPM has message reachability of 77%, DSA-Mesh has an average reachability of 67%, MENSA has an average reachability of 64%, Mobisec has message reachability of 60%, and AHKM has an average reachability of 31%. Figure 9 depicts the performance of the DAPM scheme, DSA-Mesh, and Mobisec schemes when $N_G$ is set to 10. It is observed from the figure that the average reachability of DAPM, MENSA, Mobisec, and AHKM are 68%, 64%, 64%, and 34% respectively.

According to our results analysis, the proposed DAPM's router message reachability is very high (10% to 38%) in hostile environments compared to the DSA-Mesh, MENSA, Mobisec, and AHKM schemes. In this comparison, Mobisec is a centralized key management system, and DSA-Mesh is the distributed key management system. Thus, the proposed key management mechanism has been compared with both centralized and distributed key management mechanisms. In addition to that, the proposed scheme has been compared with two other distributed key management mechanisms AHKM and MENSA.

At the end, the proposed DAPM has been compared with other existing techniques as illustrated in Table 2. In this evaluation, DAPM is experimented in its maximum network extend with number of nodes (100), attack frequency (35 malicious events/session), and network failures (10 faults/seconds). Table 2 shows the better performance of DAPM in terms of average quantities of various metrics taken through iterative simulation cycles. In this case, the proposed DAPM has 98.4% of attack detection accuracy rate. At the same time, the existing techniques are limited to multilayer authentication procedures for validating active attacks.

The average FAR and FPR are minimal for proposed model compared to existing techniques. These parameters are identified to validate the negative performance of any

Table 3: DAPM-algorithm complexity.

| Algorithms | Average computational complexity (process cycles/second) |
|---|---|
| 1.1 | 19.35 |
| 1.2 | 18.45 |
| 1.3 | 16.44 |
| 1.4 | 16.32 |

security models. Under this case, DSA-Mesh (3.11% to 3.67%) works optimally than other existing techniques. Consequently, the proposed model increases the PDR by securing both gateway and internal mesh transactions.

On the other hand, the proposed DAPM optimizes the time complexity rate at attack detection phases and overall complexity rate. Notably, the computational complexity of the proposed algorithms is illustrated in Table 3. Computational complexity is measured in terms of cycles per second. Table 3 shows the individual procedural complexity of Algorithms 1, 2, 3, and 4 in the computation domain. It shows that authentication procedures take more computational complexity than deauthentication procedures. Apart from these complexities, the attack detection rules in each router, and data transmission procedures impact the overall time complexity. The overall computation complexity in milliseconds of the proposed algorithms is illustrated in Table 2. From the overall experimental analysis, the proposed DAPM has been identified as a suitable technique for providing multilayer authentication at gateways and internal WMN nodes. Thus, the proposed system provides overall distributed security in WMN.

## 5. Conclusion

In this work, a DDoS attack prevention mechanism has been proposed for WMNs. Our proposed DAPM protects gateways and mesh routers from network attacks. The major component of this mechanism is the creation of trust among group heads using IPSec and distributed authentication and deauthentication schemes to secure the legitimate mesh nodes' join/leave operations. The distributed authentication and deauthentication algorithms protect heterogeneous devices' communication in a hostile environment. Using a binomial probability distribution model and the simulations, we prove that DAPM has better message reachability than the existing centralized and distributed key mechanisms in the backbone mesh. The overall gateway authentication and mesh router authentication procedures create a novel distributed protection against DDoS attacks, identity attacks, and reply attacks. As WMNs contain numerous internal nodes and gateway points, the crucial authentication and deauthentication are proposed by this article on round-trip transmission. This is the major contribution of the proposed model compared to existing techniques. In this regard, the implementation section shows the proposed model attains better performance than the existing techniques by 10% to 16%. Anyhow, this approach is limited to active attacks only in the mesh networks. Still, the research challenges are identified for handling more passive attacks than active attacks raised in the WMNs. On the scope, the future findings are expected to be improved with a resilient authentication model against multiple attacks in WMNs.

## Data Availability

The data used to support the findings of this study are available from the first author upon request (guncity11@gmail.com).

## Conflicts of Interest

The authors declare that they have no conflicts of interest.

## Acknowledgments

This work has been supported by the Researchers Supporting Project, King Saud University, Riyadh, Saudi Arabia, under grant number RSP-2021/250.

## References

[1] G. R. Hiertz, D. Denteneer, S. Max et al., "IEEE 802.11s: the WLAN mesh standard," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 104–111, 2010.

[2] A. F. Molisch, K. Balakrishnan, C. C. Chong et al., "IEEE 802.15. 4a channel model-final report," *IEEE P802*, vol. 15, no. 4, p. 662, 2004.

[3] D. Johnston and J. Walker, "Overview of IEEE 802.16 security," *IEEE Security & Privacy*, vol. 2, no. 3, pp. 40–48, 2004.

[4] W. Bolton, Y. Xiao, and M. Guizani, "IEEE 802.20: mobile broadband wireless access," *IEEE Wireless Communications*, vol. 14, no. 1, pp. 84–95, 2007.

[5] F. T. Akyildiz, K. Vajravelu, R. N. Mohapatra, E. Sweet, and R. A. Van Gorder, "Implicit differential equation arising in the steady flow of a Sisko fluid," *Applied Mathematics and Computation*, vol. 210, no. 1, pp. 189–196, 2009.

[6] K. G. Reddy and P. S. Thilagam, "MAC layer security issues in wireless mesh networks," in , Article ID 20028*In AIP Conference Proceedings*, vol. 1715AIP Publishing LLC.

[7] H. Bettahar, A. Bouabdallah, and Y. Challal, "AKMP: an adaptive key management protocol for secure multicast," in *In Proceedings. Eleventh International Conference on Computer Communications and Networks*, pp. 190–195, IEEE, Miami, FL, USA, 2002.

[8] J. Dong, K. Ackermann, and C. Nita-Rotaru, "Secure group communication in wireless mesh networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1563–1576, 2009.

[9] S. Routray and Q. Mao, "A context aware-based deep neural network approach for simultaneous speech denoising and dereverberation," *Neural Computing and Applications*, vol. 34, no. 12, pp. 9831–9845, 2022.

[10] F. Martignon, S. Paris, and A. Capone, "DSA-Mesh: a distributed security architecture for wireless mesh networks," *Security and Communication Networks*, vol. 4, no. 3, p. 256, 2011.

[11] V. Genc, S. Murphy, Y. Yu, and J. Murphy, "IEEE 802.16J relay-based wireless access networks: an overview," *IEEE Wireless Communications*, vol. 15, no. 5, pp. 56–63, 2008.

[12] J. Edney, W. A. Arbaugh, and W. Arbaugh, *Real 802.11 security: Wi-Fi protected access and 802.11 i*, Addison-Wesley Professional, 2004.

[13] X. Deng, T. He, L. He, J. Gui, and Q. Peng, "Performance analysis for IEEE 802.11s wireless mesh network in smart grid," *Wireless Personal Communications*, vol. 96, no. 1, pp. 1537–1555, 2017.

[14] M. Theil, M. Backhaus, M. Rossberg, and G. Schaefer, "Towards a security architecture for hybrid WMNs," in *In Proceedings of the 14th International Conference on Availability, Reliability and Security*, pp. 1–10, 2019.

[15] C. Liu and J. Qiu, "Performance study of 802.11w for preventing DoS attacks on wireless local area networks," *Wireless Personal Communications*, vol. 95, no. 2, pp. 1031–1053, 2017.

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

[17] S. Routray, A. K. Ray, and C. Mishra, "An efficient image denoising method based on principal component analysis with learned patch groups," *Signal, Image and Video Processing*, vol. 13, no. 7, pp. 1405–1412, 2019.

[18] S. Rajasoundaran, A. V. Prabu, G. S. Kumar, P. P. Malla, and S. Routray, "Secure opportunistic watchdog production in wireless sensor networks: a review," *Wireless Personal Communications*, vol. 120, no. 2, pp. 1895–1919, 2021.

[19] S. Rajasoundaran, A. V. Prabu, S. Routray et al., "Machine learning based deep job exploration and secure transactions in virtual private cloud systems," *Computers & Security*, vol. 109, article 102379, 2021.

[20] S. Rajasoundaran, A. V. Prabu, S. Routray et al., "Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks," *Computer Communications*, vol. 187, pp. 71–82, 2022.

[21] A. Gayathri, A. V. Prabu, S. Rajasoundaran et al., "Cooperative and feedback based authentic routing protocol for energy efficient IoT systems," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 11, article e6886, 2022.

[22] S. S. Kasirajan, R. M. Kumar, S. B. Manoj, S. Rajasoundaran, and P. Narayanasamy, "An analytical approach to secured routing protocol using pre-key distribution in clustered wireless sensor networks," in *In International Conference on Information Communication and Embedded Systems (ICICES2014)*, pp. 1–5, IEEE, Chennai, India, 2014.

[23] R. Soundararajan, N. Palanisamy, R. Patan, G. Nagasubramanian, and M. S. Khan, "Secure and concealed watchdog selection scheme using masked distributed selection approach in wireless sensor networks," *IET Communications*, vol. 14, no. 6, pp. 948–955, 2020.

[24] C. Thammarat and C. Techapanupreeda, "Secure key establishment protocol for smart homes based on symmetric cryptography," in *In 2022 International Conference on Information Networking (ICOIN)*, pp. 46–51, IEEE, Jeju-si, Korea, 2022.

[25] S. Iqbal and B. R. Sujatha, "Secure key management scheme for hierarchical network using combinatorial design," *Journal of Information Systems and Telecommunication (JIST)*, vol. 10, no. 37, pp. 20–27, 2022.

[26] A. Singh and K. Jain, "An efficient secure key establishment method in cluster-based sensor network," *Telecommunication Systems*, vol. 79, no. 1, pp. 3–16, 2021.

[27] S. T. Ali, V. Sivaraman, A. Dhamdhere, and D. Ostry, "Secure key loss recovery for network broadcast in single-hop wireless sensor networks," *Ad Hoc Networks*, vol. 8, no. 6, pp. 668–679, 2010.

[28] D. Sangeetha, S. Selvi, and A. Keerthana, "A trust-based handover authentication in an SDN 5G heterogeneous network," in *In Computer Networks and Inventive Communication Technologies*, pp. 841–852, Springer, Singapore, 2022.

[29] M. Kompara, S. Kumari, and M. Hölbl, "Analysis and improvement of a secure key management protocol for e-health applications," *Computers & Electrical Engineering*, vol. 73, pp. 97–113, 2019.

[30] V. Adat Vasudevan, *Secure Network Coding for Next Generation Wireless Networks [Ph.D. thesis]*, Enxeñaría telemática, 2022.

[31] S. K. Bhoi and P. M. Khilar, "SST: a secure fault-tolerant smart transportation system for vehicular ad hoc network," in *In 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*, pp. 545–550, IEEE, Solan, India, 2012.

[32] A. B. F. Khan and G. Anandharaj, "Ahkm: an improved class of hash based key management mechanism with combined solution for single hop and multi hop nodes in IoT," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 119–124, 2021.

[33] V. Bolgouras, C. Ntantogian, E. Panaousis, and C. Xenakis, "Distributed key management in microgrids," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2125–2133, 2019.

[34] R. P. Nayak, S. Sethi, S. K. Bhoi et al., "TBDDosa-MD: trust-based DDoS misbehave detection approach in software-defined vehicular network (SDVN)," *CMC-Computers, Materials & Continua*, vol. 69, no. 3, pp. 3513–3529, 2021.

[35] R. P. Nayak, S. Sethi, S. K. Bhoi et al., "TFMD-SDVN: a trust framework for misbehavior detection in the edge of software-defined vehicular network," *The Journal of Supercomputing*, vol. 78, no. 6, pp. 7948–7981, 2022.

[36] S. K. Bhoi, I. H. Faruk, and P. M. Khilar, "CSRP: a centralized secure routing protocol for mobile ad hoc network," in *In 2012 Third International Conference on Emerging Applications of Information Technology*, pp. 429–432, IEEE, Kolkata, India, 2012.

[37] Z. Yang, *A Secure and Accountable Mesh Routing Algorithm [Ph.D. thesis]*, Tufts University, 2022.

[38] S. K. Narayana and N. T. Hosur, "Priority based trust efficient routing using ant colony optimization for IoT-based mobile wireless mesh networks," *International Journal of Intelligent Engineering and Systems*, vol. 15, no. 2, 2022.

[39] K. Reddy, G. Solanki, and M. Khan, "Analysis of routing and secure routing in hybrid wireless mesh networks," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 8, pp. 2321–9653, 2020.

[40] S. K. Bhoi and P. M. Khilar, "A secure routing protocol for vehicular ad hoc network to provide ITS services," in *In 2013 International Conference on Communication and Signal Processing*, pp. 1170–1174, IEEE., Melmaruvathur, India, 2013.

[41] A. K. Roy and A. K. Khan, "Prevention against internal attack via trust-based detection for wireless mesh networks," in *In Advances in Communication and Computational Technology*, pp. 109–117, Springer, Singapore, 2021.

[42] S. K. Bhoi and P. M. Khilar, "SIR: a secure and intelligent routing protocol for vehicular ad hoc network," *IET networks*, vol. 4, no. 3, pp. 185–194, 2015.

[43] H. Bargaoui, N. Mbarek, and O. Togni, "Quality of service management in wireless mesh networks," *Service Level Management in Emerging Environments*, p. 139, 2021.

[44] U. Ghugar, J. Pradhan, S. K. Bhoi, and R. R. Sahoo, "LB-IDS: securing wireless sensor network using protocol layer trust-based intrusion detection system," *Journal of Computer Networks and Communications*, vol. 2019, Article ID 2054298, 13 pages, 2019.

[45] I. D. J. Jingle and P. M. Paul, "A collaborative defense protocol against collaborative attacks in wireless mesh networks," *International Journal of Enterprise Network Management*, vol. 12, no. 3, pp. 199–220, 2021.

[46] K. K. Jena, S. K. Bhoi, B. D. Behera, S. Panda, B. Sahu, and R. Sahu, "A trust based false message detection model for multi-unmanned aerial vehicle network," in *In 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 324–329, IEEE, Palladam, India, 2019.

[47] M. Hussain, N. Ahmed, M. Ahmed, Z. Iqubal, and N. Sarma, "QoS provisioning in wireless mesh networks: a survey," *Wireless Personal Communications*, vol. 122, no. 1, pp. 157–195, 2022.

[48] R. P. Nayak, S. Sethi, and S. K. Bhoi, "TB-EDA: a trust-based event detection algorithm to detect false events in software-defined vehicular network," in *In Intelligent Systems*, pp. 413–424, Springer, Singapore, 2021.

[49] K. Haseeb, I. U. Din, A. Almogren, N. Islam, and A. Altameem, "RTS: a robust and trusted scheme for IoT-based mobile wireless mesh networks," *IEEE Access*, vol. 8, pp. 68379–68390, 2020.