


# Modified AODV (MAODV) Against Black Hole in WMN

Geetanjali Rathee<sup>1</sup> · Hemraj Saini<sup>1</sup> 

Received: 7 November 2015/Revised: 5 February 2016/Accepted: 14 August 2017/Published online: 8 December 2017  
© The National Academy of Sciences, India 2017

**Abstract** Security for network services is a prevalent requirement against fraudulent access to the conveniences in WMN. A secure communication is indispensable for stopping the unauthorized access to the network services in wireless technology. A number of researchers have proposed various security schemes but most of them are vulnerable against several performance metrics i.e. security threats (black hole and grey hole attack), low packet delivery ratio (PDR), increased packet loss ratio (PLR) and reduced throughput. A secure routing protocol is needed in order to get rid of such precincts. In previous paper, Secured Authentication and Signature Routing (SASR) protocol proposed a secure signature routing protocol which provides the communication using Diffie Hellman and threshold signature. In this manuscript, SASR is enhanced with AV-SASR (Advanced Version of SASR) by modifying AODV (MAODV) protocol which is robust against black hole and grey hole attack. Further network metrics are measured in terms of PDR, PLR and throughput in comparison of SAODV and SEAODV. The analysis is done over both the scenarios i.e. with the involvement of malicious node and without involvement of malicious nodes.

**Keywords** Wireless mesh network · Diffie Hellman · AV-SASR · Secure packet transmission · Threshold signature technique · MAODV

## 1 Introduction

Wireless mesh network (WMN) [1] has been developed as an eminent concept to overcome the problems of adaptive re-configurable architecture [2] with the reasonable cost effective emulsion. The architecture of WMN comprises of Mesh Routers (MRs) and Mesh Clients (MCs). WMN with multi hop mesh routers acts as wireless backbone from which some are deployed as gateway routers (which are connect to the internet by wired backbone) and are usually stationary whereas MCs are the end user devices which employ the network services and are generally dynamic in nature.

Presently, there exist three types of WMN, (i) *Client WMN* where mesh clients may unnervingly communicate with each other without engrossment of MR's. (ii) *Infrastructure based WMN* in which clients may access the services through mesh router's and (iii) *Hybrid WMN* [3] which is a mishmash of previous two. As hybrid architecture of WMN is expedient in catastrophe recovery phase but it may not perform well for wide coverage cities. Infrastructure based is best known WMN where clients may directly connected through routers up to large coverage areas. As WMN has become gradually a prevailing replacement technology for last mile connectivity to the community and family networking, it is domineering to design a safe and proficient communication protocol. In WMN, security can be easily conceded due to its distributed, broadcasting and dynamic nature. Therefore, an ornate authentication mechanism [4, 5] and a secure

✉ Hemraj Saini  
hemraj1977@yahoo.co.in

Geetanjali Rathee  
geetanjali.rathee123@gmail.com

<sup>1</sup> Department of Computer Science and Engineering, Jaypee University of Information Technology, Wagnaghat, Solan, India

routing [6, 7] should be indispensable to assure that only trusted nodes have access to various amenities with efficient network performance.

The existing secure routing protocols i.e. SAODV [8], AODV-CGW [9] and SEAODV [10] cannot adopt well in heterogeneous environment of WMN due to its dynamic and broadcasting nature and causes passive eavesdropping and decrease in network metrics i.e. end to end delay and packet loss ratio. Further these protocols are vulnerable to a variety of security threats i.e. black hole and grey hole attacks [11, 12]. One of the severe hitches in IEEE 802.11 WMN is the design of apt secure routing protocol which can handle unpredictable vigorous topological variations and multi-hop transmission of broadband facilities. Smooth provision of broadband facilities over a multi-hop mainstay is a stimulating task and is one of the foremost reasons of recital degradation [13] i.e. poor packet delivery ratio (PDR) and security threats in WMN.

However, to prevent from these loopholes, a secure routing is needed. A previous work has been carried out for secure authentication and signature routing protocol (SASR) [14] for reducing computational overhead and response time. The proposed protocol validates the authenticity of mesh nodes efficiently and overlays the way for secure communication using Diffie Hellman key exchange protocol which reduces the bandwidth allocation for the key. Due to dynamic nature of WMN and involvement of number of intermediate mesh routers during communication between source and destination, there is chance of involvement of security threats from passive traffic analysis to DOS, black hole, grey hole attacks and makes the design of WMN a challenging issue. In this paper, the previously proposed algorithm is enhanced by modifying AODV protocol which is resilient against black hole and grey hole attacks. Further the network metrics are discussed by considering both the cases (i.e. with the involvement of malicious nodes and without the involvement of malicious nodes) in the network.

### 1.1 Manuscript Contribution

Some amendments are made to the AODV [15] routing protocol in order to address security threats (black hole and grey hole) and improve the network performance in terms of packet delivery ratio (PDR), throughput and packet loss ratio (PLR) in infrastructure based WMN. The modified AODV protocol is merged with previous SASR approach to further enhance the security process. The Advanced-Version of SASR (AV-SASR) is analyzed using both the scenarios i.e. malicious and non-malicious nodes. The key contribution of AV-SASR is discussed as follows:

1. A modification on AODV routing protocol is done called MAODV by utilizing the static nature of mesh routers.
2. To ensure the safety, proposed mechanism retains the information of its 2-hop previous node in order to judge the legitimacy of the node and identify black hole and grey hole attacks in WMN.
3. To further proliferate the security level, MAODV is merged with SASR which is capable of securing communicating data packets within and between the domain networks during communication. Proposed approach i.e. AV-SASR is robust against several security threats and enhances the network metrics inside the network.

## 2 Related Work

The singular characteristic [16] of WMN not only assists the users but also invites the number of vulnerabilities to come. The below text discusses some characteristics of WMN with their cons:

*Anywhere Anytime* The anytime joining of a network from anywhere may allow the end users to access the internet services with maximum flexibility and freedom but these selves of WMN not only ease the mesh clients but also offers enough scope to a rival to launch safety threats from anywhere and anytime.

*Multi-hop Characteristics* To surge the coverage range of WMN with easy deployment and network flexibility, multi-hop characteristic is important parameter in WMN. As the number of hops increases between source and destination, severe performance degradation ensues such as bandwidth reduction, security threats etc. Further the multi-hop characteristic of WMN may involve a number of routing attacks i.e. black hole and grey hole attacks.

*Dynamic Nature* Due to the dynamic nature of mesh clients, an attacker may access the network services by forging the address of a legitimate client. So to remove this limitation a strong authentication is needed for stopping the unauthorized access of network services.

In order to overcome these limitations, a number of researchers have proposed various security protocols i.e. SAODV [8] is a protected version of AODV protocol which uses hash chains and digital signatures to implement the security inside the network. Hash chains are used to secure the hop counts in the routing packets field while digital signature secures the routing messages. In this, originating node initiates the route discovery process by engendering Time To Live (TTL) value and seed number

**Table 1** Existing security schemes

Protocol	Aim	Pros	Cons
SAODV [8]	Proposed security through hash chains and digital signatures	Secure routing messages and packet fields inside the network	Passes issued by third party broker
AODV-CGA [9]	Forward the data packets through closest access point in WMN	Protocol is transparent to the user	Vulnerable against active attacks
SEAODV [10]	Authenticate unicast messages in the network	Fast and Secure	Vulnerable against computational overhead
EAP-TLS [17, 18]	Providing authentication solution for WMN	Independent of the technology of wireless media	Requires IP addresses in mesh nodes which lead to several active attacks
FPBPKD [19]	Proposed a 4-way handshake pro-active key distribution	Copes up against corrupted Transit Access Point (TAPs) security problems	Security issues exist in the backbone network
LHAP [20]	Provide mobile client authentication in wireless dynamic environment	Prevents resource consumption attacks	Leads to high computational overhead
LAAA [23]	Provides continuous, on-demand, end-to-end security in heterogeneous networks	Establish a central point of contact for service providers	Vulnerable against user privacy concerns

with maximum Hop count. SAODV is robust against modification of hop count and sequence number attacks but does not provide hop by hop authentication.

Although SAODV prevents the hop count filed in routing messages from decreasing but attacker may still increase the hop count to affect the routing decision of the node. Furthermore it fortifies the routing messages but does not assure the authentication and integrity of the packets coming from a node.

AODV-CGA [9] which is an addition of AODV routing protocol designed to forward the data packets to the adjoining one in the incidence of numerous access points in WMN. The access points are associated with gateways that are liable for joining the points to the internet. The basic idea of AODV-CGA is connection of altered access points under a conjoint gateway. The author claims that the AODV-CGA is translucent to the nodes.

SEAODV [10] is another secure routing protocol proposed for WMN. It is based on Pre-Distribution Keys PDK which compute the secret pairwise transient key PTK i.e. RREP (Route Reply) to authenticate the unicast messages and Group Transient Key GTK to authenticate the broadcast messages i.e. RREQ (Route Request). MAC are used to ensure the authenticity and integrity of the messages in order to provide security in hop by hop manner. But the protocol is vulnerable against computation and communication overhead. EAP-TLS [17, 18] protocol proposed by Simon provides the authentication solution for WMN independent of the wireless media technology. But it requires an IP address in mesh node which leads to several active attacks.

FPBPKD [19] proposed a 4-way handshake pro-active key distribution mechanism which copes up against corrupted transit access points but is vulnerable against

security issues that exist in the backbone network i.e. network congestion and communication delay.

An LHAP [20] which is a WMN security protocol is proposed to provide the mobile clients authentication [21, 22] in dynamic environment but leads to heavy computational overhead. Further LAAA [23] provides a constant on-demand end to end safety in heterogeneous networks by establishing a central point for service providers. Table 1 shows the listed security schemes with their cons.

Due to unique characteristic of WMN, prevailing routing protocols must be reconsidered to make them attuned with WMN environment by considering some important issues:

1. Gateways and mesh routers are stationary.
2. Clients may be mobile or static in nature.
3. WMN can be Influential against security threats.
4. Network performance [24, 25] should not degrade with the involvement of security protocols.

### 3 SASR Protocol

This section illustrates a brief introduction of previously proposed SASR approach with its model. In SASR, a hierarchical WMN architecture is taken to consist of three different layers, i.e. internet layer (top layer) which provides the services to the end users, mesh router layer (intermediate layer) through which services are provided and mesh client's layer (bottom layer) which accesses the services. Internet gateways are used to provide the connectivity, traffic is forwarded by mesh routers and finally wireless devices access the network services (as shown in

Fig. 1). To prevent unauthorized access of network services and passive analysis of transmitting packets from source to destination, a strong authentication is needed. In previous work, authentication in SASR is provided using key distribution and inter-cluster processes as shown in Table 2. The detailed summary of SASR is discussed in [14].

### 3.1 Model of SASR

SASR uses shared secret key for node’s authentication and threshold signature using HMAC for bootstrapping the trust. Shared secret key is also called symmetric cryptology which provides the authenticity to the nodes by a single key between source and destination using Diffie Hellman key exchange algorithm and Threshold signature is used to maintain the trust relationship between the nodes. SASR uses threshold signature where each node sends a message tuple to the verifier ‘v’ and cluster head of the domain. A proposed model of SASR is depicted in Fig. 2.

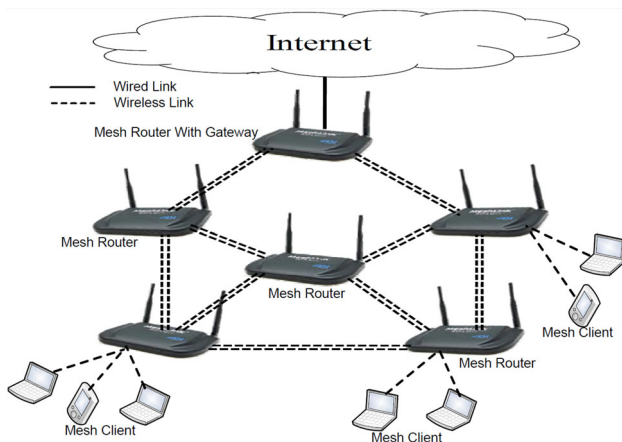


Fig. 1 Wireless mesh network

In this, during cluster header format, circle is formed by calculating the mean of points within the circle after choosing a node as a center. For Cluster head selection, clustered nodes are formed based on trust values. Authentication Technique starts with the threshold generation. The complete process of Threshold signature generation is described in Table 3. In order to generate a threshold signature for message N, a number of S2 (b1, b2, b3, b4, b5) nodes including the members of node perform the following steps.

As WMN is dynamic in nature (any node may enter or leave the network at any time), so it is necessary to establish trust between them. The aim of threshold signature generation is to establish trust among the nodes inside the network.

The algorithm of Secure Packet Transmission of SASR protocol (i.e. SPT for SASR) is shown below and explains the complete execution of SASR in both the cases i.e. during inter-domain or intra-domain communication.

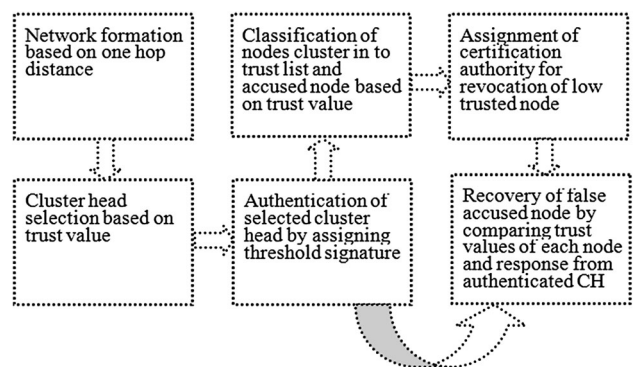


Fig. 2 Network model of SASR

Table 2 Authentication process

Key distribution	Each zonal Mesh Router MR and Mesh Client MC agree on a shared key $K_s$ using diffie Hellman key algorithm and a cluster shared key $\{kc_{1,2}; kc_{1,3}; kc_{2,3} \dots kc_{m,n}\}$ is used to agree with adjacent zone’s MR. The shared key of zones varies reliant on the number of adjacent zones
Inter-zone communication	Let us consider a source MC ‘Sr’ in a zone desires to connect with an adjacent zones destination Mesh Client ‘Dn’. In this, communication is provided using shared secret keys of respective zones and cluster shared keys of adjacent zones
Authentication process	<p>Step 1: To access the receipt node, sender ‘sr’ will create a random number <math>r_1</math> to compute the requesting code ‘rc’. Sender ‘sr’ will pass ‘rc’ as a request to receiver as a authentication verification initialization</p> <p>Step 2: Receiver will propel another created random number <math>r_2</math> to the sender. The authentication vector <math>AV^c</math> will be generated by sender as a response. To complete the verification process, <math>AV^c</math> will be sent at receiver side</p> <p>If <math>AV^c</math> of sender and receiver are same, then { authentication satisfied Else Not valid}</p>

**Algorithm (SPT algorithm for SASR)****Assumptions:**

1. For inter communication, each zone needs to agree on a cluster head ZMR between ZMR<sub>i</sub> and ZMR<sub>j</sub> through KC<sub>m,n</sub>
2. For intra communication, each MC<sub>i</sub> needs to agree with MR<sub>i</sub> through a shared key K<sub>sn</sub>
3. AODV routing protocol is used for communication

**Abbreviations:**

ZMR- Zonal Mesh Router

KC<sub>m, n</sub>- Cluster shared key between m and n

MC- Mesh Client

N- Total number of nodes in the network

**Input:** source client MC<sub>i</sub> wants to communicate with the destination client MC<sub>j</sub>**Output:** Secure packet transmission between MC<sub>i</sub> and MC<sub>j</sub>**Algorithm steps**

1. If Mesh client MC<sub>i</sub> wants to communicate with destination client MC<sub>j</sub>  
Then Check the type of communication
  2. If (inter domain communication)  
Then Go to step 3  
Else  
Go to step 4
  3. **//Inter domain communication**  
Start  
For (i=0; i<N; i++) {
    - i. MC<sub>i</sub> encrypts the message using shared key K<sub>sn</sub> and send it to the next node using AODV routing protocol
    - ii. If (intermediate node) {  
Packet transferred to the next node  
Else (destination node)  
MC<sub>j</sub> decrypt the message and verify the authenticity of the message
    - iii. If (message authenticated)  
Communication successful  
Else  
Attacker encountered and simply drop the packet  
}
4. **//intra domain communication**  
Start  
For (i=0; i<N; i++) {
  - i. Source client MC<sub>i</sub> transmits the packet to the zonal ZMR<sub>i</sub> after encrypting it with the shared key
  - ii. ZMR<sub>i</sub> decrypt the message and re-encrypt it with the clustered key KC<sub>m,n</sub> and send it to the adjacent zone MR i.e. ZMR<sub>j</sub>
  - iii. ZMR<sub>j</sub> decrypt the message using same cluster key and send it to the destination client MC<sub>j</sub> after re-encrypt it with its zonal shared key K<sub>sn</sub>
  - iv. Destination client MC<sub>j</sub> see the message after decrypting it with its shared key ks
  - v. If (message authenticated) {  
Communication successful  
Else  
Attack encountered and simply drops the packet  
}

**Table 3** Generation process of threshold signature

In order to generate a threshold signature for message N, a number of S2 (b<sub>1</sub>, b<sub>2</sub>, b<sub>3</sub>, b<sub>4</sub>, b<sub>5</sub>) nodes including the members of Node perform the following steps

Step 1: Primarily, all member nodes request for threshold signature. This is underway by one of the signers by convincing a threshold generation request to selected CH along with list of signers as (TK<sub>1</sub>... TK<sub>S<sub>2</sub></sub>)

Step 2: Nodes send tokens. For this CH selects a random token  $T_R \in Z^*_q$  where,  $1 \leq R \leq S_2$  and sends them to the corresponding signers very securely

Step 3: After that each signer creates a signature:  $sig_{PKR} = H_0(N).K_{PKR}$  and calculates the signature with a corresponding token:  
 $T.sig_{PKR} = TA.sig_{PKR}$

Step 4: Later nodes start sending signature along with pseudonym public key. Here, each node sends the message tuple to the verifier V and CHj.  
 (N, Q<sub>PKR</sub>, Q<sub>PK1</sub>, T\*sig<sub>PKR</sub>, HMAC<sub>PKR</sub> (M,Q<sub>PKV</sub>,T.sig<sub>PKA</sub>))

The further section introducing a new work to reduce security threats i.e. black hole and grey hole attacks in WMN.

### 4 MAODV (Modified AODV Routing Protocol)

#### 4.1 Assumptions and Designing Strategy

We assume that the mesh routers and gateways are static in nature. Gateways are associated with the internet and mesh routers form a backbone by concerning with each other. Mesh clients are directly linked with end points mesh routers as shown in Fig. 1.

The architecture of WMN is hierarchical in nature. As discussed earlier, the top layer constitutes the internet which provides the services to the end users through multi-hop mesh routers. Mesh routers form the intermediate level of static backbone while mesh clients contribute at the lower level which utilizes the network services. The mesh clients forward the packets to the gateways through numerous mesh routers as shown in Fig. 3.

The designing base of SASR routing protocol is based on the MAODV distance vector algorithm in which all the nodes keep the information of 2-hop preceding neighbor due to overhearing quality. The algorithm pursuits for the shortest route between source and destination using Bellman Ford routing algorithm.

#### 4.2 Routing Table and Route Discovery Phase

Generally, Routing Table encloses the information as destination address, next hop address, routing cost and its

**Table 4** Neighboring Information of MR-B

1-Hop Neighbor	2-Hop Neighbor	2-Hop Neighbor	2-Hop Neighbor
MR-A	1	–	–
MR-E	4	5	–
MR-C	6	7	8

metric used. In MAODV, routing table contains one additional information regarding the neighbors of its 2-hop neighbor as shown in Table 4.

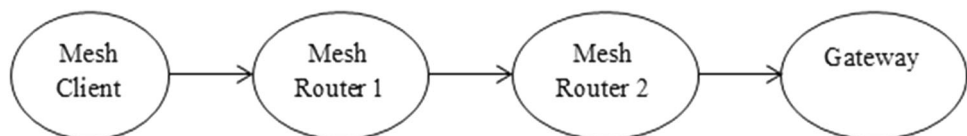
Let us consider node 5 wants to link with node 8 as depicted in Fig. 4. Node 5 will initiate a RREQ message through MR-E. The MR-E will now multicast the RREQ to all its neighbor routers i.e. MR-B. The MR-B will re-multicast the request to its neighboring node to further discover the route to destination node. The final establishment of path from source to destination is E-B-C.

#### 4.3 MAODV

To best understand the routing communication of proposed protocol, let us consider a scenario where source node S wants to communicate with destination node D. The approach is explained by taking both the scenarios i.e. without the involvement of security threats and with the involvement of security threats.

Let source node S needs to propel the data packets to destination D through MR1-MR2-MR3 (as depicted in Fig. 5) path, then each node will check the validity of its preceding node using Preceding Node Validity (PNV) as given in Eq. 1.

**Fig. 3** WMN communication hierarchy



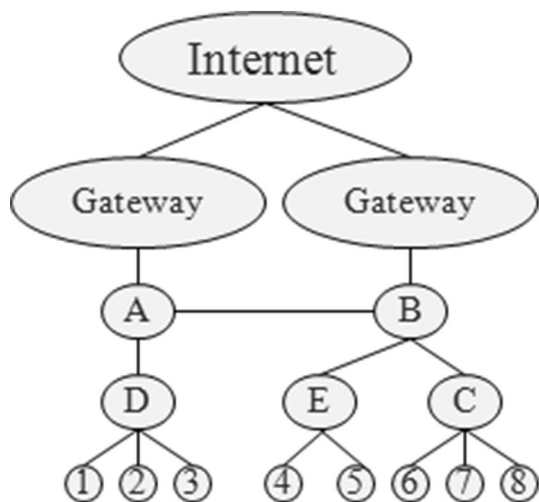


Fig. 4 Packet flow in MAODV

$$PNV = \frac{\text{Packets Received by Current Node}}{\text{Packets Received by Previous Node}} \tag{1}$$

If the PNV value is satisfying the threshold ratio, then previous node is valid else current node will check the packets received by its 2-hop preceding node to checks that its preceding node is valid or not. So, each current node checks the validity of its preceding node by calculating the PNV value. Let source node conveys 250 packets to destination node, each node will forward all the packets if they not malicious nodes. If a node receives less number of packets then there exists two kinds of possibilities either packets are dropped due to network congestion or packets are dropped by black hole and grey hole attacks.

To clearly understand the difference between these two cases, network has set some assumptions.

If a node has received 75% of total generating packets that means packet drop ratio is due to network congestion. So, the current node will immediately send an alarm message to its preceding node only to slow down the packet transmission process. If packets received by current node are less than 75% that means there is a chance of black hole and grey hole attacks i.e. if PNV value calculated by the current node is less than 75%, there are the chances of security threats. The current node will immediately generate an alarm to its 2-hop preceding node to inform that its preceding node is either grey hole or black

hole. 2-hop preceding node will immediately change the route to destination node to prevent from these attacks.

4.3.1 Case 1: Without Involvement of Malicious Node

Let source node S sends 250 packets to MR1 and MR1 has received all 250 packets. Now, to check the validity of its preceding node (i.e. source node), node 1 will calculate PNV ratio as given in Eq. 2.

$$Node\ s = \frac{250(node1)}{250(node\ s)} \tag{2}$$

The PNV value of node S is 1 that means node S is legitimate node. Now, node 1 will send 250 packets to node 2. The packets received by node 2 are 250. Node 2 will check the PNV of node 1 as: Node 1 = (250 (node 2))/(250 (node 1)) = 1. The same procedure will be followed by all the nodes. By following this procedure, each node checks the validity of its preceding node.

4.3.2 Case 2: With the Involvement of Malicious Node

Let node 2 is malicious (as depicted in Fig. 6). Node S has sent 250 packets to node 1. Likewise node 1 has sent 250 packets to node 2. Now, as node 2 is malicious node so, packets forwarded by node 2 are less than 250 as given in Eq. 3. Let node 2 has dropped 25% of packets and has forward only 75% (i.e. 175).

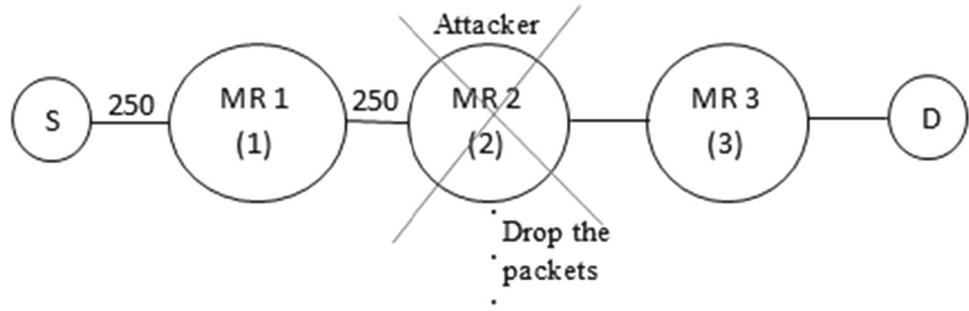
$$Node2 = \frac{230(node3)}{250(node2)} \tag{3}$$

As node 3 calculates the PNV ratio of node 2 which is less than threshold value that means node 2 is not a legitimate node. To further confirm whether the less number of packets received by node 3 are due to network congestion or drop by an attacker, node 3 will overhear node 2 preceding node i.e. node 1. If the packets sent by node 1 are 250 that means node 2 is malicious node and will immediately send an alarm message to node 1 as a malicious node alarm. Node 1 will immediately stop forwarding the remaining packets to node 2 and will follow another route through Bellman Ford algorithm. If packets are less than 250 at node 1 also, then packets are lost due to traffic congestion, node 3 will send an alarm to node 2 to slow down the packet forwarding process.

Fig. 5 Packet transmission in MAODV



**Fig. 6** Packet transmission in MAODV



**Table 5** Authentication and designing policies of network and security of SASR

Assumptions and goals	Explanation
Network assumption and designing goal	Wireless network links are bidirectional i.e. if node A can hear node B then node B can also hear node A as depicted in Fig. 7. The threshold signature technique is used to provide strong authentication and trust management among the nodes
Security assumption	A shared secret key is used for intra-communication while cluster shared key is used for inter-communication
Security designing goals	Provide network authentication and reduction of end to end authentication delay

### 5 Performance Details

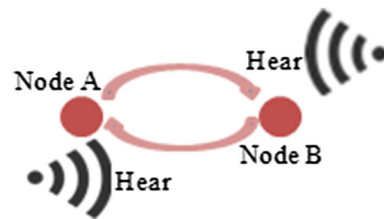
This section discusses the performance analysis of both the protocol independently (i.e. SASR and AV-SASR). SASR describes the formal analysis of performance while metrics are measured in AV-SASR protocol.

In order to simplify our discussion, SASR describes two kinds of goals, i.e. security and network. Each goal has its own assumptions and designing policies (as shown in Table 5). The main objective of this manuscript is to discuss the authentication and trust management requirements of SASR and analyze the experimental results against network parameters with the involvement of security threats.

#### 5.1 Formal Analysis

##### 5.1.1 Authentication and Designing Policies of Network and Security of SASR

Verification of the authenticity of each node is necessary for securing the network. Each security protocol has to satisfy the authentication requirements, i.e. efficiency, for decreasing end to end authentication delay; a protocol should not incur a large bandwidth and must be resource efficient. Scalability achieves when computational cost does not increase with the network size. Transparency ensures the independence of the protocols means turn off or on of one protocol should not affect the functionality of other protocols. Packet delivery ratio defines that on applying security protocol with routing protocol, there



**Fig. 7** Bidirectional link

should not be any effect on the packet delivery ratio and finally throughput must increase on applying security protocol.

##### 5.1.2 Nodes Authentication and Trust Management

The aim of this subsection is to describe how nodes are authenticated and a trust is maintained among communication nodes. The *Node Authentication* mechanism used by SASR is based upon Diffie Hellman key exchange algorithm. In this, a node only authenticates each other within its domain and each MR and MC has a separate shared secret key. So, it is hard for an invader to launch an attack. While Trust Management comprises trust bootstrapping, trust maintenance and trust termination. *Trust bootstrapping* is done when a node joins a network; it first needs to agree on a shared key 'ks' for intra-communication and cluster shared key (KCs) for inter-communication. Furthermore, trust bootstrapping is done within the zone and between the zones.



In trust bootstrap within the zone, MC and MR need to agree on shared secret key  $K_s$ . Let us assume that a node  $S$  wants to communicate with a node  $D$  within a zone. Then source node  $S$  will follow the procedure as (4) and (5) while in Trust bootstrap between the zones, the node needs to agree on a cluster secret key  $K_c$ . If a node  $S$  within a zone wants to communicate with another zone's node  $D$  then the following procedure needs to be followed in (6–8).

$$\text{source} \xrightarrow{\text{encrypt}(K_{ns}(\text{message}))} \text{zonal Mesh Router} \quad (4)$$

$$\text{Mesh Router} \xrightarrow{\text{decrypt}(K_{ns}(\text{message}))} \text{Destination} \quad (5)$$

$$\text{source} \xrightarrow{\text{encrypt}(K_{ns}(\text{message}))} \text{zonal Mesh Router} \quad (6)$$

*zonal Mesh Router decrypt*

$$(KC_{m,n}(\text{message})) \xrightarrow{\text{encrypt}(KC_{m,n}(\text{message}))} \text{zonal Mesh Router} \quad (7)$$

*zonal Mesh Router decrypt*

$$(KC_{m,n}(\text{message})) \xrightarrow{\text{encrypt}(K_{n,s}(\text{message}))} \text{source} \quad (8)$$

After that, *Trust maintenance* is done using the generation of pseudonyms and authentication techniques (as discussed in [14]). Further moving to Trust termination, in SASR there exists two scenarios underneath trust relationship between nodes will be terminated. The first is when a compromised node is detected during internal communication and another is if a node calculates the trust value between two nodes during zonal communication.

## 5.2 Performance Metrics

The further study of SASR approach focuses on performance metrics in which computational overhead and authentication delay problems are solved by using threshold signature and Diffie Hellman techniques. Several security and network metrics are carried out for the analysis. The research on these metrics proves the pros and properties of WMN security based on cluster based threshold signature technique. Further by adding an extra security protocol with SASR i.e. AV-SASR it is resilient against many routing attacks i.e. black hole and grey hole attacks. Black hole attack is the one in which a compromised node offers itself as the shortest route to reach the destination so that it can drop the entire packet flow going towards it. While in grey hole attack, malicious node selectively forwards the packets to destination node. These two attacks are taken as severe attacks in the network as they cause a large delay and packet drop ratio inside the network. These two spams can be alleviated using AV-SASR by observance its important features i.e. 2-hop

neighbor information and PNV. Further Diffie Hellman algorithm and HMAC may enhance the routing security inside the network.

Both grey hole and black hole attacks can be mitigated using AV-SASR by keeping in view its important features i.e. privacy of data packets using HMAC or Diffie Hellman key exchange algorithm and security threats using PNV and neighbor nodes information. As each client or mesh router keeps the 2-hop neighbor information in its routing table, so, it is not possible for an attacker to drop the packets going towards it while PNV resist against both grey hole and black hole attacks. Current node checks the maliciousness of its preceding node as its preceding node is grey or black hole.

As discussed earlier, in black hole attack, malicious node drops the entire packets coming towards it while grey hole drops selective packets. For e.g., route from  $S$  to  $D$  is  $S$ -MR1-MR2-MR3- $D$ , here let us suppose node 2 is black hole. The PNV value of node 2 (MR2) will be zero as it simply drops the entire packets and will not forward any packet to its next hop while in grey hole attack the PNV value would be less than threshold value as it may drop some selective packets. Now, AV-SASR is resilient against these attacks as node 3 may check the validity of its preceding node by calculating the PNV value, if node 3 calculates the PNV value of node 2 and would find less than threshold value, it would immediately send an alarm message to node 2 to stop forwarding the remaining packets.

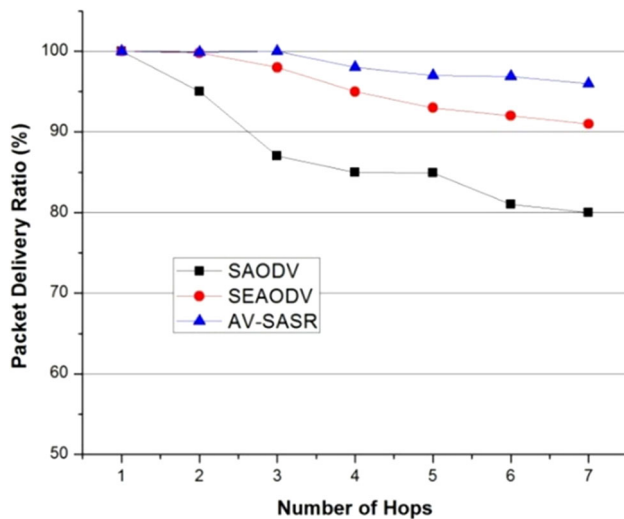
## 5.3 Performance Evaluation with Simulation Results

1. *Packet delivery ratio (PDR)* is the ratio of packets received by destination to number of packets sent by source node.
2. *Packet loss ratio (PLR)* is the loss of packets in the presence of an attack.
3. *Computational Cost* is defined as the time taken by the source node to rifle and confirm the path to destination node.
4. *Throughput* is calculated as the time required transmitting the total number of packets to destination node.

The simulation graph of the whole network is done in ns2. A fixed delay and transmission is used, i.e. 120 m/s and hop count of 250 m by distributing the nodes randomly at 500\*500 area square. All the mobile nodes are equipped with IEEE 802.11 and 2 Mbps data rate. The Source node generates CBR traffic with a packet size of 512 bytes. Every node in our network has to run our algorithm to become a Cluster Head. A random 200 and 300 s are chosen as life time of keys. Here, we measure different

**Table 6** Simulation parameters

Parameters	Size
Number of nodes	200
Area size	500*500
MAC	802.11
Routing protocol	MAODV
Simulation time	50 s
Traffic source	CBR
Packet size	512 bytes
Antenna	Omni Antenna

**Fig. 8** Packet delivery ratio versus number of hops

networking parameters of proposed secure routing protocols. Table 6 shows the simulation parameters and in order to simplify our discussion the figure of each metric is explained and proves the validity of the proposed work.

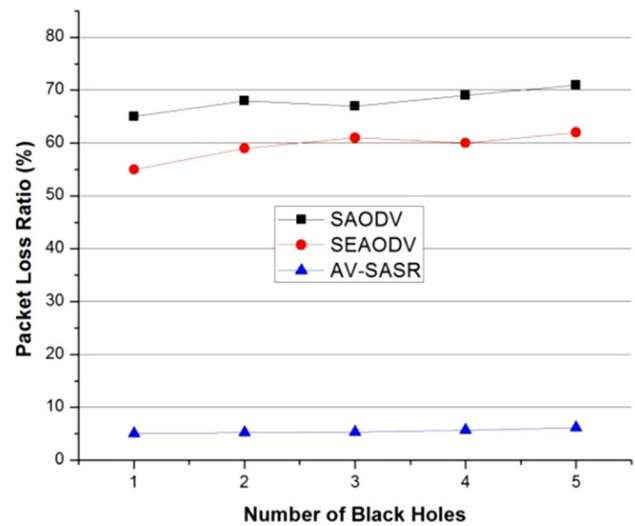
The metrics listed below compare the performance security and reliability of AV-SASR with both the existing protocols i.e. SEAODV and SAODV.

### 5.3.1 Packet Delivery Ratio (PDR)

The PDR for SAODV, SEAODV and AV-SASR are shown in Fig. 8. AV-SASR outperforms SAODV and SEAODV. The PDR of AV-SASR is approximately 100% till the three hops and slightly drops to 96% when number of hops further increase. SEAODV achieves 100% up to 2 hops and the ratio between 98 and 91 for remaining 7 hops while SAODV performance significantly drops and PDR drops to 80%.

### 5.3.2 Analysis of PDR Graph

The simulation observed that as the number of nodes increase, SAODV PDR is plumed. The reason is that

**Fig. 9** Packet loss ratio versus number of black hole

SAODV and SEAODV are based on on-demand routing protocols where route will be established only when needed. As the number of nodes increase, the proven route will be longer which may enhance the possibility of security attacks (i.e. black/grey hole) which results in reduced packet delivery. While in case of AV-SASR, delivery ratio increased due to overhearing quality and PNV value which identifies the attack and prevents immediately.

### 5.3.3 Packet Loss Ratio (PLR)

The grey hole and black hole attack are introduced in network to obtain PLR statistics. The below graph (Fig. 9) depicts the graph comparison.

### 5.3.4 Analysis of PLR Graph

In order to obtain PLR statistics, a black hole is introduced because of its most severe property. AV-SASR has 95% delivery rate with the existence of 5 black hole attacks. The drop ratio of packets is only 5% as compared to SEAODV (having 28% packet drop ratio) as shown in Fig. 9. The reason is that, AV-SASR identifies and prevents from black hole attack due to its important features (PNV and 2-hop neighbor information).

### 5.3.5 Computational Cost with Analysis

Figure 10 shows the graphs of computational cost between SAODV and AV-SASR. The computational cost of SAODV is much higher in comparison of AV-SASR. The reason is that, SAODV needs to calculate the digital signature and hash functions which may increase the computational cost, while AV-SASR uses shared secret keys to

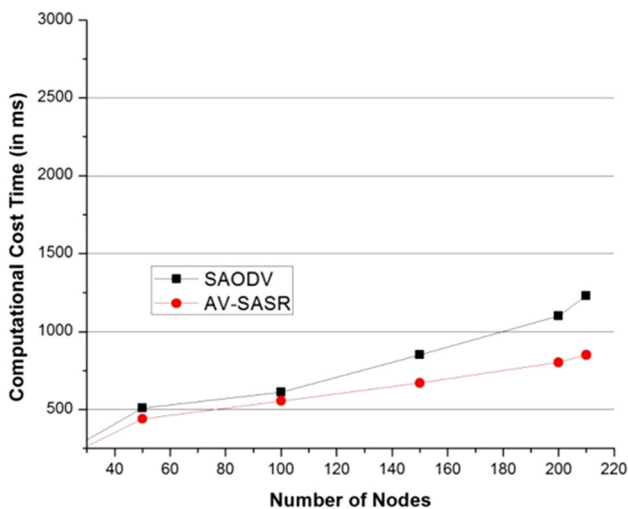


Fig. 10 Computational cost for SAODV and AV-SASR

secure the transmitting packets and trust among the nodes establish a secure and quick route between source and destination.

### 5.3.6 Throughput

To compute throughput scenario with and without malicious node, Figs. 11 and 12 observe that without introducing any black hole or grey hole attack, AV-SASR achieves 99.8%, SEAODV achieves 98.7% and SAODV achieves 98% throughput. While after introducing black hole attack throughput ratio drops to 97.9% in case of AV-SASR and 92% in SEAODV.

The obtained statistics show the importance of AV-SASR and validate its efficiency in the large scale hostile environment of WMN.

## 5.4 Formal Analysis of AV-SASR

After modifying the AODV routing protocol, AV-SASR obtained better results than existing approaches in terms of PDR, PLR, Computational cost and throughput. The below text describes some formal analysis of AV-SASR.

### 5.4.1 AV-SASR is Resilient against Security Threats

SAODV and SEAODV provide the security with some extension but suffer from security threats. AV-SASR is resilient against black hole or grey hole attacks after a little modification in standard AODV routing protocol.

### 5.4.2 Resistant against Packet Modification

As an attacker may alter the packets transmitted between source and destination even during a security protocol (i.e.

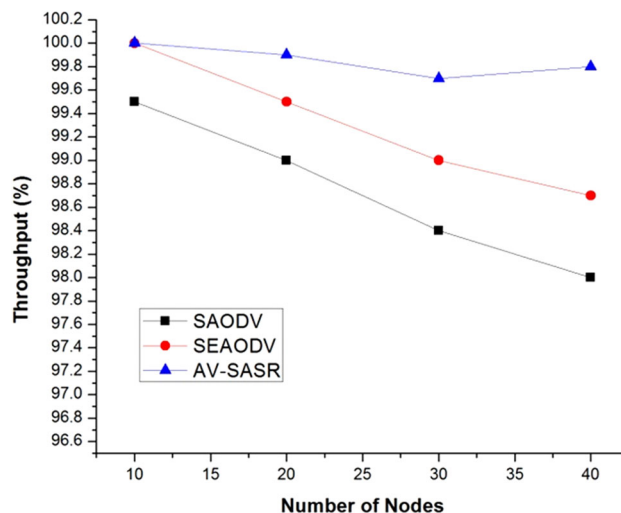


Fig. 11 Throughput versus network size

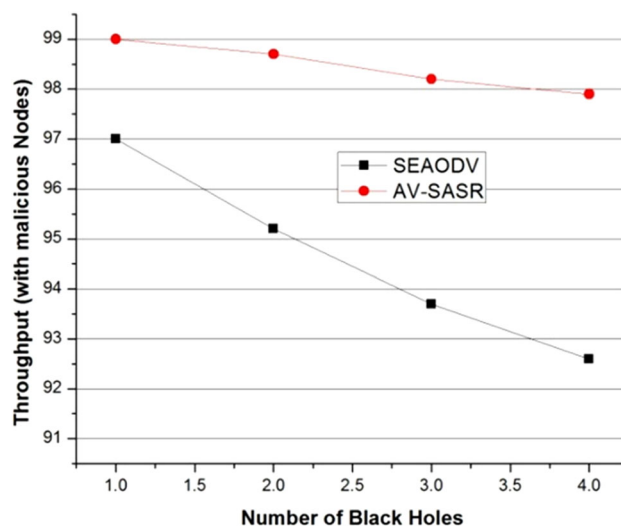


Fig. 12 Throughput versus number of black holes

SAODV), proposed protocol AV-SASR is resilient against packet modification due to encryption of transmitted message with cluster or shared keys.

### 5.4.3 Trust Among the Backbone Mesh Routers

Due to dynamic and broadcasting characteristic of WMN, it is necessary to establish a trust among the communicating nodes; AV-SASR also establishes trust among the nodes through threshold signature protocol.

### 5.4.4 Communication Overhead

Existing security protocols (SEAODV) provide the security with increased communication overhead. AV-SASR protocol is also resilient against this issue due to its efficient security mechanism.

### 5.4.5 Better Network Performance

A security protocol is good only if it is transparent with any other protocol i.e. if security protocol is added with existing routing procedure then there may be a chance of reduced network degradation. Proposed AV-SASR provides the security with enhanced network metrics.

## 6 Conclusion and Future Work

In this manuscript, the design and evaluation of MAODV routing protocol is presented and merged with SASR i.e. AV-SASR, a secure infrastructure based WMN routing protocol which uses MAODV routing. Due to dynamic and broadcasting nature of WMN, security is the utmost concern of all the networks. In this paper, AODV protocol is altered with MAODV for avoiding the security threats. The previously proposed protocol i.e. SASR is merged with MAODV to prevent packet modification and security threats. In proposed MAODV, the Preceding Node Validity (PNV) and 2-hop neighbor flag concept are introduced in the routing table of each access point and client to create an efficient routing against black/grey hole attack. In order to prove the efficiency of proposed protocol, network metrics are measured and compared against existing protocols by describing both the scenarios (with the involvement of black/grey hole attack and without the involvement of security threats). In future work, we plan to consider some modifications in MAODV routing protocol to identify more security threats i.e. jelly fish, worm hole and Byzantine attacks.

## References

1. Akyildiz IF, Wang X (2005) A survey on wireless mesh networks. *IEEE Commun Mag* 43:23–30
2. Bicket J, Aguayo D, Biswas S, Morris R (2005) Architecture and evaluation of an unplanned 802.11b mesh network. In: *Proceedings of 11th conference on mobile computing and networking*, New York, vol 1, pp 31–42
3. Mir S, Pirzada A, Portmann M (2008) HOVER: hybrid on-demand distance vector routing for wireless mesh networks. In: *Proceedings of the thirty-first Australasian conference on computer science*, Australian Computer Society, pp 63–71
4. Khan K, Muhammad A (2006) Authentication in multi-hop wireless mesh networks. In: *Transactions on engineering, computing and technology*, pp 178–183
5. Lin X, Ling X, Zhu H, Ho P, Shen X (2008) A novel localized authentication scheme in IEEE 802.11 based wireless mesh networks. *Int J Secur Netw* 3:122–132
6. Rathee G, Rakesh N (2013) Resilient packet transmission for buffer base routing protocol. *J Inf Process Syst*. doi: [10.3745/JIPS.03.0014](https://doi.org/10.3745/JIPS.03.0014)
7. Zapata MG (2008) Secure routing in wireless mesh networks, security in wireless mesh networks. CRC Press, New York
8. Lu S, Li L, Lam KY, Jia L (2009) SAODV: a MANET routing protocol that can withstand black hole attack. In: *IEEE international conference on computational intelligence*, pp 421–425
9. Asherson S, Hutchison A (2006) Secure routing in wireless mesh networks. In: *Proceedings southern African telecommunication networks and applications conference*, Spier Wine Estate, Stellenbosch, South Africa (2006)
10. Li C, Wang Z, Yang C (2010) SEAODV: a security enhanced AODV routing protocol for wireless mesh networks. In: *Transactions on computational science XI*. Springer, Berlin, Heidelberg, pp 1–16
11. Cai J, Yi P, Chen J, Wang Z, Liu N (2010) An adaptive approach to detecting black and gray hole attacks in ad hoc network. In: *24th IEEE international conference on advanced information networking and applications (AINA)*, pp 775–780
12. Baumann R, Heimlicher S, Lenders V, May M (2007) HEAT: scalable routing in wireless mesh networks using temperature fields. In: *IEEE international symposium on world of wireless, mobile and multimedia networks, WoWMoM*, pp 1–9
13. Rathee G, Mundra A, Rakesh N (2013) Buffered based routing and resiliency approach for WMN. In: *IEEE international conference on human computer interactions*, Chennai, India, pp 1–7
14. Rathee G, Saini H, Ghrera SP (2016) Secured authentication and signature routing protocol for WMN (SASR). In: *Proceedings of the second international conference on computer and communication technologies*. Springer India, pp 327–336
15. Chakeres ID, Belding E (2004) AODV routing protocol implementation design. In: *Proceedings of 24th international conference on distributed computing systems workshops*, pp 698–703
16. Subramanian A, Buddhikot M, Miller S (2006) Interference aware routing in multi-radio wireless mesh networks. In: *2nd IEEE workshop on wireless mesh networks*, pp 55–63
17. Tseng YM (2009) USIM-based EAP-TLS authentication protocol for wireless local area networks. *J Comput Stand Interfaces* 31:128–136
18. Aboba B, Blunk L, Vollbrecht J, Carlson J, Levkowetz H (2004) Extensible authentication protocol (EAP), RFC No. 3748
19. Kassab M, Belghith A, Bonnin J, Sassi S (2005) Fast pre-authentication based on proactive key distribution for 802.11 infrastructure networks. In: *Proceedings of the 1st ACM workshop on wireless multimedia networking and performance modeling*, pp 46–53
20. Zhu S, Xu S, Setia S, Jajodia S (2003) LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks. In: *Proceedings of 23rd international conference on distributed computing systems workshops*, pp 749–755
21. Miller SP, Neuman BC, Schiller JI, Saltzer JH (1987) Kerberos authentication and authorization system. In: *Project athena technical plan*
22. Debiao H, Jianhua C, Jin H (2012) An ID-based client authentication with key agreement protocol for mobile client-server environment on ECC with provable security. *J Inf Fusion* 13:223–230
23. Prasad N, Alam M, Ruggieri M (2004) Light-weight AAA infrastructure for mobility support across heterogeneous networks. *J Wirel Pers Commun* 29:205–219
24. Shaw WT, Wong SW, Cheng N, Balasubramanian K, Zhu X, Maier M, Kazovsky LG (2007) Hybrid architecture and integrated routing in a scalable optical-wireless access network. *J Lightwave Technol* 25:3443–3451
25. Passos D, Teixeira DV, Muchaluat DC, Magalhaes LCS, Albuquerque C (2006) Mesh network performance measurements. In: *International information and telecommunications technologies symposium*, pp 48–55