Journal of Scientific & Industrial Research
Vol. 81, October 2022, pp. 1061-1072
DOI: 10.56042/jsir.v81i10.57471

Prevention of Blackhole Attack in MANET using Certificateless Signature Scheme

Vimal Kumar[1], Mahima Shanker[2], Aanjey Mani Tripathi[1], Vikash Yadav[3]*, Anjani Kumar Rai[4], Uzair Khan[5] & Mayur Rahul[6]

[1]School of Computing Science and Engineering, Galgotias University, Greater Noida 201 310, UP, India
[2]Babu Banarasi Das Institute of Technology & Management, Lucknow 226 028, UP, India
[3]Government Polytechnic Bighapur Unnao, Board of Technical Education, Bighapur 209 865 UP, India
[4]Departement of CEA, GLA University, Mathura 281 406, UP, India
[5]ABES Engineering College, Ghaziabad 201 009, UP, India
[6]Department of Computer Application, CSJM University, Kanpur 208 024, UP, India

Received 22 November 2021; revised 26 September 2022; accepted 27 September 2022

Mobile AdHoc Networks (MANETs) are the network of self-configuring nodes. Such nodes communicate through single as well as multi-hop modes without the aid of any centralized administrator or pre-existing network infrastructure. Due to this reason, MANETs have gained a highly significance in modern wireless networking technologies. Such networks are extremely vulnerable to one of the security attack i.e. blackhole attack. It is a malicious node when an attacker is able to send a fake route reply to the originator of a route request packet. Such attackers discard the legitimate packets and replay packets in the whole network thereby adversely affecting network performance. Most of the security protocols for MANET are using bilinear pairing methods to provide security against security attacks and it takes high computing cost for the computation of pairing operations. Nowadays, researchers are using certificate-less signature schemes in distributed environments to provide efficient security. This signature scheme is very popular because it does not use any certificate authority for the management of security certificates. In this paper, we proposed an efficient technique to prevent blackhole attack in MANET using RSA-based certificateless signature scheme without using any bilinear pairing operations. Our scheme provides security against forgery and blackhole attacks and is evaluated under a discrete logarithm problem. Proposed scheme outperforms existing schemes in terms of these metrics viz., throughput, packet delivery ratio, routing overhead and end-to-end delay when we are varying mobility and fixed percentage of malicious nodes. Our proposed scheme not only detects or prevents the blackhole attack but it is also capable to provide important security services viz., integrity, authentication and non-repudiation.

Keywords: Ad hoc network, AODV, Malicious, Route discovery, RSA

Introduction

MANETs[1–3] are more popular due their critical applications in various areas, viz., medical services and logistics through horticulture, education, sensor network, ranger service, entertainment, common and development building, to reconnaissance and military applications. In such a network, each mobile node forms a self-organized, self-creating and self-directing wireless network. Nodes of such networks communicate in single-hop/multi-hop manner using an infrastructure-less network. Development of a routing protocol[4] in MANET is a very tough task due to unique feature i.e. dynamic topology. Reactive i.e. on-demand routing protocol and proactive i.e. table driven are two broad categories of routing protocol[4] in MANET. A routing table is updated through use of periodic message exchange in such protocol. MANETs have various security challenges[5–7] due to lack of pre-existing fixed infrastructure, dynamic topology and broadcast nature for communication between two nodes. There are various security attacks concentrating on vulnerabilities in routing protocols of MANETs. One of the most vulnerable attacks is blackhole in such networks.[8] Vehicular Ad hoc Networks fraction of MANET, which states that each node i.e. vehicle can move any direction within the stay connected and network coverage. Each node can commune to other nodes in multi-hop or single-hop manner.

Security Requirements: There are some basic security requirements[9,10] or secure communication are as follows:

*Author for Correspondence
E-mail: vikas.yadav.cs@gmail.com

***Confidentiality*:** A message has confidently when it protects from disclosure or exposure to unauthorized entities. It ensures that only an entity is able to access information. If an unauthorized entity can view the message that is known as confidentiality is compromised.

***Authentication*:** This means that message is imminent from trusted authority and going to the authorized claimed destination node.

Integrity: A message has integrity when it is complete, whole, and uncorrupted. It means that a transmitted message is never modified by an unauthorized party.

***Non-repudiation*:** It makes sure that after sending or receiving a message, communication parties can never deny.

AODV Protocol: Ad-hoc On-demand Distance Vector (AODV)[11–13] is the most popular routing protocol for MANETs. Each node has to maintain a routing table for storing routing information about available paths in the network. This information is used to find a path when a sender S wants to send some data to the desired receiver; firstly, it checks paths in the routing table. If a path exists in such a routing table then it sends a data packet along with its route to the originator node. Mobile nodes start a route discovery method by sending a Route Request (RREQ) packet all over the network if they don't already have a route to the desired destination. Upon receiving a route request message, all participating mobile nodes check whether they have a desired path or not, if they have a path then it sends a Route Reply (RREP) packet to an originator of RREQ message, otherwise they forward RREQ message to their neighbours node.

A network scenario consists of seven mobile nodes and one malicious node, which is shown in Fig. 1. Here, a sender S; it wants to send some data to a receiver D. Therefore, S is not having any path to D, so it broadcasts a RREQ message in the entire network. All the participating mobile nodes check whether they have the desired path. If a fresh path is available in routing table then they forward reply using RREP message to the corresponding source node (S), otherwise they forward a RREQ message to neighbours node. Here, Packet format of route request message is < originator address i.e. OA, originator sequence number i.e. OSN, RREQ-ID, destination address i.e. DA, destination sequence number i.e. Dseq, hop count i.e. H >. Destination node (D) forwards route reply (RREP) message of

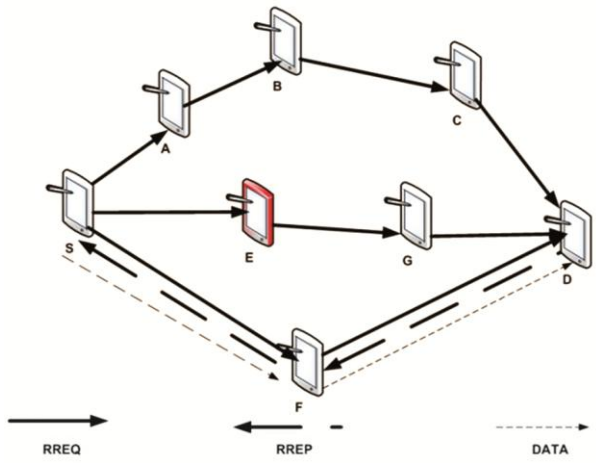

Fig. 1 — AODV protocol in MANET

corresponding RREQ message. S gets a first RREP message from a malicious node E. D can get more than one RREQ for the same broadcast id. So, D responds to the very first RREQ and discards the rest of RREQ for the same broadcast id. Packet format of RREP message is: < originator addresses i.e. OA, destination address i.e. DA, destination sequence number i.e. Dseq, hop count i.e. H, lifetime i.e. LT >.

***Blackhole Attack in AODV Protocol*:** AODV is used to locate a route for sending some data to a desired destination in the networks. Here, an attacker is available in the networks. When an attacker receives a RREQ message, it gives a prompt response i.e. fake RREP message having a high destination sequence number. Upon receiving a RREP message, the sender node finds a fresh path through a fake RREP message. Such a path is a fake one because an attacker sent it. Sender node sends data packet via attacker node. Such an attacker is able to drop all data packets without forwarding a destination node. This is known as blackhole attack.[14–16]

A destination sequence number[17,18] has length of 32 bits arithmetic i.e. 232 bits long. An attacker performs two types of fabrication in a RREP message; first fabrication is sending a highest destination sequence number while second one is lower hop count. Upon receiving a fabricated message, source node selects a path whose hop count is low and destination sequence number is high. Here, a combination of low hop count and high destination sequence number shows a fresh route in the networks. A sender (S) wants to send some data packet to a receiver (D), which is shown in Fig. 2. It uses route discovery mechanism to find the path. When an intruder node (E) gets a RREQ message, then it sends a route reply with high value of

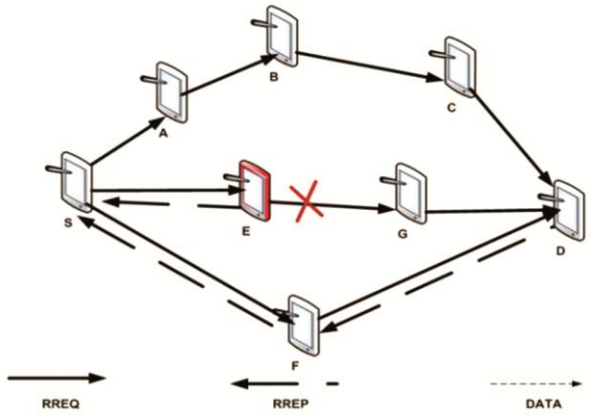

Fig. 2 — Blackhole attack

destination sequence number and low value of hop count to the sender node (S). Such a node claims that it has the shortest path to a destination node D. When node S gets route reply message from node E, it transmits data node E, which is able to drop/delete data[19] i.e. sent by node S. Tamilselvan *et al.*[20] introduced a fidelity table which is able to counter the blackhole attack in MANETs. It uses fidelity level to assign every participant in the network. If the fidelity level of a mobile node drops toward zero i.e. known as a malicious node under a blackhole attack otherwise known as legitimate one. Main disadvantage of this scheme is having high value of end-to-end delay.

Panda *et al.*[21] gave a key authentication mechanism to prevent malicious nodes in MANET. It carries a routing table to all participant mobile nodes in the networks. For key generation, a pseudo code is used then a trust value is calculated using comparison of both keys. If outcome appears zero then it is known as a malicious node, otherwise known as legitimate one. It has high end-to-end delays due to the key generation process.

Zapata *et al.*[22] introduced a secure AODV (SAODV) routing protocol. Such routing protocol applies a digital signature in diverse fields i.e. RREQ, RREP packet and hash chain. An originator of a message is signed on by its own private/public key and after that it sends to a destination node. SAODV has a problem with key distribution in MANET.

Raj *et al.*[23] gave a novel prevention, detection and reactive routing protocol AODV i.e. DPRAODV. It is used to prevent malicious nodes under blackhole attack when an incident is notified by participating nodes.

Hu *et al.*[24] introduced a security in on-demand ad-hoc network i.e. Ariadne routing protocol. It protects from malicious routes that route consists of uncompromised nodes. This routing protocol uses symmetric cryptography primitives.

Kurosawa *et al.*[25] gave a novel technique i.e. anomaly based detection. Such a scheme uses a dynamic training method for updating of training data, which is done at an orderly time interval.

Deng and *et al.*[26] developed an algorithm to prevent AODV routing protocol from blackhole attack. According to this technique, when a sender node receives an RREP packet, it checks with the following mobile node in its path for a different route. A bogus RREP packet is one that has no route to the receiving node from the following mobile node. This method's significant end-to-end delay and routing overhead are its key drawbacks.

Ghosh *et al.*[27] gave an approach to prevent AODV routing protocol from blackhole attack in MANETs. In this approach, a trust field is added with a RREQ packet, and a trust field is modified by an intermediate mobile node. This work is on a trust based mechanism and this method has no delay but it has computation and routing overhead.

Gajera *et al.*[28] gave an approach to prevent AODV routing protocol from blackhole attack. It uses a threshold and a cryptography based mechanism. An attacker node cannot be entered in the network because an attacker node is unaware of the security mechanism of network. This work is based on a cryptography mechanism and this method has computation overhead and routing overhead with no delay.

Jaiswal *et al.*[29] gave a technique to prevent a network from blackhole attack. It is based on the destination sequence number of sender and receiver nodes. A source node collects all route reply and discards first reply if DSN is very high as compared to source sequence number (SSN). A route network is opted by a source based on remaining RREPs. This work is based on sequence number mechanism and this method has only computation overhead with no delay and routing overhead.

Maheshwar *et al.*[30] gave an algorithm for prevention of blackhole attack. This algorithm is known as an intrusion prevention system. This work is based on intrusion detection based mechanism and this method has only computation overhead with no delay and routing overhead.

Singh *et al.*[31] gave a scheme to prevent AODV from blackhole attack. Here, all RREP packets are collected at a sender node and destination sequence

number (DSN) of all RREP messages are compared with SSN. If the DSN of any RREP is very high then it is discarded. This work is based on sequence number mechanism and this method has high computation overhead and delay but no routing overhead.

Kumar *et al.*[32] gave a novel CLS scheme that prevents MANET from blackhole attack. It uses a bilinear pairing method that takes a high computation cost. This scheme has high routing overhead.

All the above existing schemes involve additional overhead on either/both destination and intermediate nodes in one or the other way. These schemes do not provide any security mechanism. Since the mobile nodes in mobile ad hoc networks suffer from processing power, limited battery life, and storage, it is essential to devise a protocol that aims to detect and mitigate blackhole attack in the presence of malicious nodes.

Author's Contribution: We present an RSA based signature scheme without using any bilinear pairing operations. Salient features of proposed scheme as follows:

- Presented signature scheme introduces some out of the many applications of the proposed signature scheme in MANET, VANET and Flying AdHoc Network (FANET).
- Such a scheme provides security against forgery and blackhole attacks.
- It outperforms existing schemes in terms of these metrics viz., throughput, packet delivery ratio, routing overhead and end-to-end delay when we increase the percentage of malicious nodes under fixed mobility of nodes.
- It provides some important security services viz., integrity, authentication and non-repudiation.
- It outperforms existing schemes in terms of the above metrics when we are varying mobility under a fixed percentage of malicious nodes.
- It also provides secure data communication in the existence of malicious mobile nodes.

Materials and Methods

Network Model: Here, a cluster based mobile ad hoc network is used as shown in Fig. 3.

There are some beliefs are as follows:

- Each cluster consists of mobile nodes and one cluster head (CH).
- Each node has a unique identity.
- A CH performs data communication and allocation of resources to all mobile nodes in a particular cluster.

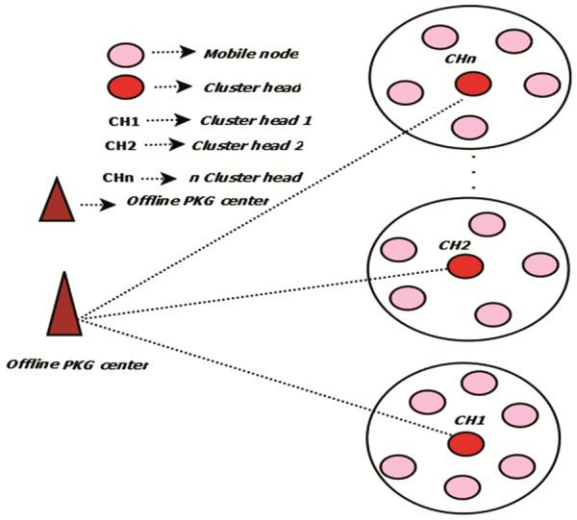

Fig. 3 — Network model

Table 1 — System parameters

x	Prime number
y	Prime number
d	Master secret key
e	Public key
n	Here $n = p \times q$
M_{Pub}	Public key
M_{Prv}	Private key
$\phi(n)$	Euler totient function
$Param$	System parameter
$H_0(\ )$	Mapping from $\{0,1\} \rightarrow Z_n^*$
$H(\ )$	Mapping from $Z_n^1 \times \{0,1\}^e \rightarrow \{0,1\}^s$

- We take an offline PKG center[33] that performs some basic functions such as setup phase, private/public key generation and verification.

Phases used in proposed model are as follows:

- Setup
- Key generation
- Sign generation
- Communication
- Verification

Setup phase: There is one cluster head per cluster. The system parameters are depicted in Table 1.

Algorithm 1: Setup Phase

INPUT: 1^k

Ensure: {s, d and param}

1. Select two relatively large prime number x' and y
2. Find the value of $x \leftarrow 2x' + 1$

3. Find the value of $y \leftarrow 2y' + 1$
4. Compute $n \leftarrow (x \times y)$
5. Compute $\phi(n) \leftarrow (x-1) \times (y-1)$
6. $e.d = 1 \bmod \phi(n)$
7. Choose two hash functions $H()$ and $H_0()$
8. Compute hash value $H_0(): \{0,1\}^* \rightarrow Z_n^*$
9. Find the hash value $H(): Z_n^4 \times \{0,1\}^* \rightarrow \{0,1\}^s$
10. Find system parameter

$Param \leftarrow (\{H(), H_0(), e, n\})$

A cluster head performs the following operations:

A cluster head broadcasts the system parameters $Param = \{H(), H_0(), e, n\}$ in the entire cluster, which is depicted in Fig. 2.

Key Generation Phase

All mobile nodes have to send their identity to a corresponding cluster head when it receives system parameters.

Cluster head forwards identity to the KGC.

i. After that KGC generates public/private key using Algorithm 2.

Algorithm 2: Public/private key generation phase

INPUT: {Param, d and ID}

Ensure: $\{M_{Pub}, M_{Prv}\}$

1. **for** *i =1 to N* **do**
2. $M_{Pub_i} \leftarrow H_0(ID_i)$
3. **end for**
4. **for** *i =1 to N* **do**
5. $M_{Prv_i} \leftarrow (M_{Pub_i} \times x \times d)$
6. **end for**
7. KGC preloads the public/private key.
8. KGC sends private key to mobile node via cluster head

i. **Public Key**: A KGC generates public key for all the mobile nodes are as follows:

Public key: $Pub_{key_i} = H_0(ID_i)$

Where $0 \le i \le n$

ii. **Private Key**: A KGC generates private key are as follows:

Private Key: $\Pr_{key_i} = Pub_{key_i} \times p \times d$

Where $0 \le i \le n$

iii. A KGC sends private key to all participants using a secure medium.

Signature Generation Phase

A mobile node wants to secure data communication in the network. Such a node generates a signature using Algorithm 3.

Algorithm 3: Signature generation phase

INPUT: $\{Param, M_{Prv}, ID\}$

Ensure: ρ

1. Choose two prime number i.e. N_1 and N_2
2. **for** *i =1 to N* **do**
3. Compute $A_{1i} \leftarrow H_0(ID)^{N_1} \bmod n$
4. Find $A_{2i} \leftarrow \left| H_0(ID)^e \right|^{N_2} \bmod n$
5. $h \leftarrow H\left(A_{1i} \,||\, A_{2i} \,||\, ID_i \,||\, M \,||\, M_{Pub_i}\right)$
6. Compute $U_{1i} \leftarrow \left[H_0(ID_i)^{d(N_1-h)}\right]$
7. Compute $U_{2i} \leftarrow (N_2 - eh)$
8. **end for**
9. Compute $\alpha \leftarrow \left(U_{1i} \,||\, U_{2i} \,||\, h \,||\, M\right)$

Verification Phase

We use the following steps to verify the signature:

a. Here, CH works as a verifier in our scheme. When CH receives appended RREP with signature i.e. σ . Correctness of a signature scheme on route reply packet is as follows:

i. $R_1^! = u_1^e H_0(ID)^{eh} \bmod n$

ii. $R_2^! = H_0(ID)^{u_2} Pub_{key}^{(\Pr_{key} \times h)} \bmod n$

iii. $h^! = H(R_1^!, ID, R_2^!, Pub_{key,} M)$

b. A cluster head checks following condition:

$h = h^!$

$h = H(u_1^e H_0(ID)^{eh} \bmod n, H_0(ID)^{u_2}$

$Pub_{key}^{(\Pr_{key} \times h)} \bmod n, ID, Pub_{key}, M)$

c. If the above condition holds then i.e. a valid signature, otherwise a fake signature.

Correctness of Proposed Signature Scheme

Correctness proposed signature is as follows: We know that a verifier checks the conditions $h = h^!$. If above condition is true then it is known as a valid signature otherwise a fake one.

$h^! = H(u_1^e H_0(ID)^{eh} \bmod n, H_0(ID)^{u2}$

$Pub_{key}^{(\Pr_{key} \times h)} \bmod n, ID, Pub_{key}, M)$

$= H((H_0(ID)^{C_1 - h})^e H_0(ID)^{eh} \bmod n,$

$H_0(ID)^{C_2 - (\Pr_{key} \times h)} H_0(ID)^{(\Pr_{key} \times h)} \bmod n,$

$ID, Pub_{key}, M)$

$$= H\begin{pmatrix} H_0(ID)^{C_1 e-eh} H_0(ID)^{eh} \bmod n, \\ H_0(ID)^{C_2} \bmod n, ID, Pub_{key,} M \end{pmatrix}$$

$$= H\left(H_0(ID)^{C_1 e} \bmod n, R_2, ID, Pub_{key}, M\right)$$

$$= H\left(\left(H_0(ID)^{e}\right)^{C_1} \bmod n, R_2, ID, Pub_{key}, M\right)$$

$$= H\left(R_1, R_2, ID, Pub_{key}, M\right)$$

$$= h$$

Algorithm 4: Signature verification phase
INPUT: {Param, M, ID, σ }
Ensure: True or False

1. μ selects two prime number i.e. N_1 and N_2
2. **for** *i =1 to N* **do**
3. Find $A_{1i} \leftarrow H_0(ID)^{N_1} \bmod n$
4. Find $A_{2i} \leftarrow \left[H_0(ID)^{e}\right]^{N_2} \bmod n$
5. $h \leftarrow H(A_{1i} \| A_{2i1} \| ID_i \| M \| M_{Pub_i})$
6. Find $U_{1i} \leftarrow \left[H_0(ID_i)^{d(N_i - h)}\right]$
7. Find $U_{2i} \leftarrow (N_2 - eh)$
8. **end for**
9. Find $\sigma \leftarrow \left(U_{1i} \| U_{2i} \| h \| M\right)$

Communication Phase

In this subsection, we divide communication phase into two sub-phases i.e. secure communication in inter and intra cluster.

*a. **Secure Communication in Intra Cluster***

Secure communication in intra cluster is following:

i. A sender (S) sends a RREQ packet to a corresponding cluster head to find a path for the target node in Fig. 4.
ii. Cluster head forwards a RREQ packet to the running cluster. If a mobile node sends RREP without a signature to CH, such route reply is considered as a fake route reply and it is discarded by the cluster head.
iii. Upon receiving route request packet from the cluster head, node (B) sends a fake route reply packet without a signature of an originator of the route request. Such a node does not have a secret key. The fake secret key is used to create a signature on route reply packet.
iv. A cluster head creates a public/private key pair of the originator of an RREP packet using Algorithm 2.

Public Key: $M_{Pub_{black}} \leftarrow H_0(ID_i)$

Private Key: $M_{black_{\Pr v}} \leftarrow \left(M_{Pub_i} \times x \times d\right)$

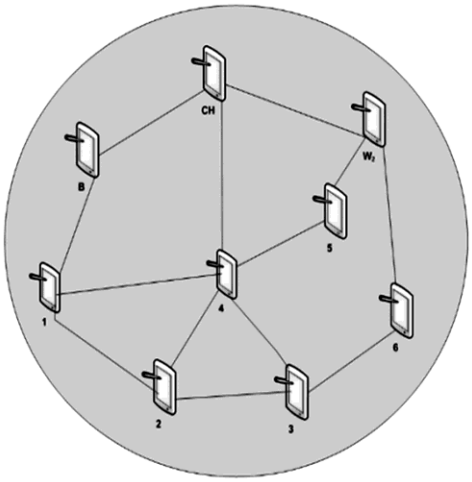

Fig. 4 — Intra cluster communication

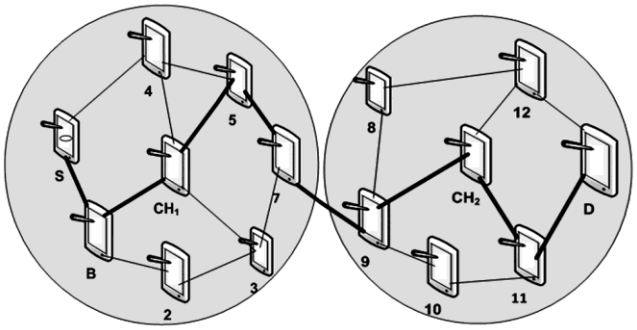

Fig. 5 — Inter cluster communication

v. When cluster head receives a fake signature on route reply packet then it verifies the above signature

Secure Communication in Inter Cluster

A source node (S) in the presence of blackhole (B)[34–37] is shown in cluster C_1 and destination node resides in cluster C_2 which is depicted in Fig. 5.

The steps used in communication in inter-cluster are as follows:

i. A sender (S) unicasts a RREQ packet to corresponding cluster head to find a path for destination and it waits a response from the cluster head.
ii. When a node receives a route request from node (S), the running cluster is informed by CH of the request.
iii. A blackhole node creates a fake signature on a RREP packet without having a fresh route to a receiver and sends it to the S.
iv. After that cluster head verifies the coming route reply using verification phase.

Let assume, a malicious node (B) creates a false signature for distribution of communication between *CH* and mobile nodes. Such node creates a fake public key i.e. $M_{Pub_{fake}}$ and a private key i.e. $M_{\Pr v_{fake}}$. We use flowchart for prevention of malicious nodes under blackhole attack, which is depicted in Fig. 6. When a replying node receive RREQ packet then it appends signature with $(\sigma_{fake}, Dest_{Seqno}) + RREP$ to a corresponding *CH*. A cluster head computes the following values:

i. $R_1^{!} = u_1^{e} H_0(ID)^{eh} \bmod n$

ii. $R_2^{!} = H_0(ID)^{u_2} (M_{Pub_{fake}})^{\left(M_{\Pr v_{fake}} \times h\right)} \bmod n$

iii. $h^{!} = H(R_1^{!}, R_2^{!}, ID, M_{Pub_{fake}}, M)$

A cluster head checks the condition $h = h^{!}$ using Algorithm 3. If a given condition holds then it is known a valid signature otherwise, it is considered a fake signature.

$h^{!} = H(u_1^{e} H_0(ID)^{eh} \bmod n, H_0(ID)^{u_2}$

$M_{Pub_{fake}}{}^{M_{\Pr v} \times h} \bmod n, ID, M_{Pub_{fake}}, M)$

$h^{!} \neq h$

$L.H.S \neq R.H.S$

Hence, it shows that our scheme detects when malicious node performs blackhole attack in the networks. If above condition is true then it is known as legitimate reply, otherwise fake reply.

Algorithm I is used to prevent blackhole attack in MANET. Notations used in Algorithm I has been represented in the Table 2. They use following steps:

Algorithm I: Prevention against Blackhole Attack

Step 1: All the participants of the running cluster use the setup phase.

Step 2: Source node transmits a route request to the running cluster:

$SN(RREQ) \Rightarrow C$

Step 3: For each RREP [i] do

// Check the following condition:

if $\left(Dest_{reply\_node} > Dest_{RREQ}\right)$ then

// Replying node creates signature and it appends with RREP then it sends to the running cluster head.

reply node (*signature on RREP) ==> CH*

Step 4: *CH* applies the signature verification phase using Algorithm 3.

if (h = h$^{!}$)

It is referred as a legitimate route reply.

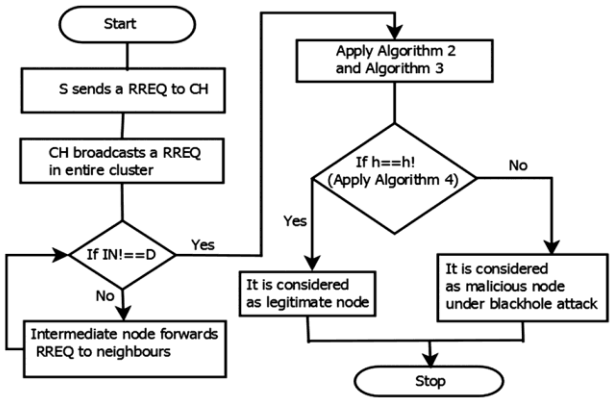

Fig. 6 — Flow chart for prevention of blackhole attack Security Analysis

Table 2 — Notations

SN	Source Node
$Dest_{RREQ}$	Destination sequence number of originator of RREQ
$Dest_{reply\_node}$	Destination sequence number of originator of route reply
S_{CH}	Signature of cluster head
C	Cluster

// Cluster head creates its own signature and it appends with RREP then finally it sends to the source node.

CH sends (signature on *RREP*) ==> *SN*

else

It is known as a blackhole attack.

Step 5: A signature on route reply consists combination of (σ , *RREP*).

Step 6: *Source node (SN)* decrypts signature on *RREP and gets the desired path*

Step 7: *Source node (SN)* this route for a secure communication in MANET

Performance Evaluation

We have proposed an RSA based signature scheme to prevent malicious nodes under blackhole attack in MANET.[38–44] Performance evaluation has been completed using a network simulator (ns-2).We use some notations in our scheme which is depicted in Table 3. A snapshot of the simulation scenario is depicted in Fig. 7.

Performance metricsA performance evaluation of proposed and the existing schemes has been made using the following performance metrics.

Packet Delivery Ratio (PDR): It is the proportion of all packets sent from one end to another and all packets received at the receiving end. Here, $PKTR_i$ represents

Table 3 — Simulation Parameters

Terms	Value
Simulator	ns-2
Mobility Model	Random waypoint model
Simulation area	500×500
Routing protocols	AODV, SAODV
Simulation Time	600 s
Pause time	6 s
Packet Size	512 bytes
Number of nodes	10 to 80
Speed of Traffic agent	15 m/s
Transmission range	250 m
Speed of mobile node	2–9 m/s
Percentage of blackhole node (Malicious node)	0 to 50%

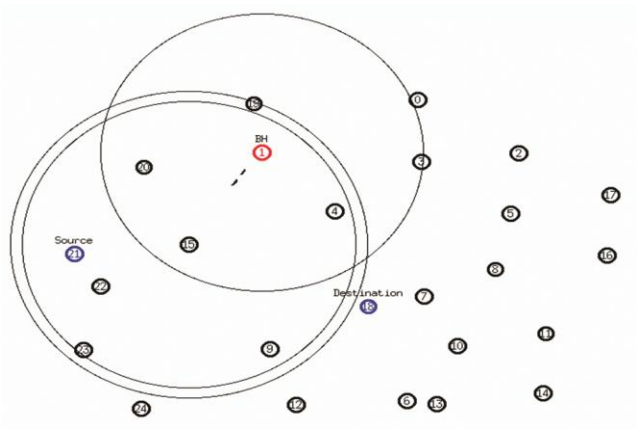

Fig. 7 — A snapshot of the simulation scenario

the total amount of packets received at the receiver end, and $PKTS_i$ represents the total number of packets sent by the sender end in the i^{th} interval. For n application traffics, we calculate PDR value as follows:

$$PDR = \sum_{i=1}^{n} \frac{PKTR_i}{PKTS_i}$$

End-to-end delay (E_{delay}): It measures the ratio between the sender and recipient ends for an average packet to be properly transmitted. Here, PKT_{total} denotes total amount of the packets received by a destination end while $delay_i$ represents total delay of packets received by a receiver end. For n application traffics, we calculate PDR value as follows:

$$E_{delay} = \sum_{i=1}^{n} \frac{delay_i}{PKT_{total}}$$

Throughput (Th): It is a ratio of total amount of data ($Total_{data}$) at destination end received from a source end and total time (Total time) for destination end gets the final packets. It defines the total amount of data packets transmitted per second. We can calculate throughput for the n application traffic is as follows:

$$Th = \sum_{i=1}^{n} \frac{Total_{data}}{Total_{time}}$$

Routing overhead ($R_{overhead}$): It measures the proportion of all data transmissions to total control packet transmissions. Here, the ith interval is employed to transmit the total amount of control packets ($CPKT_i$) and total number of data packets (PKT_{total}). Following is a formula we may use to get the routing overhead for the n application traffic:

$$R_{overhead} = \sum_{i=1}^{n} \frac{CPKT_i}{PKT_{total}}$$

We are considering only two scenarios, viz., scenario 1 and scenario 2.

Scenario 1: Affects performance metrics when varying number of malicious nodes under a fixed mobility in the network.

Scenario 2: Affects performance metrics when varying mobility of nodes with fixed malicious nodes in the networks.

Results and Discussion

Scenario 1: Effect on performance metrics when varying number of malicious nodes under a fixed mobility.

From simulation results, it shows that packet delivery ratio is better in our scheme as compared to existing schemes, viz., standard AODV[4], SAODV[22] and CLS[32] scheme as depicted in Fig. 8. It observed that PDR degrades when we are increasing the percentage of malicious nodes under blackhole attack. Our scheme has 96.93% while standard AODV[4], SAODV[22] and CLS[32] scheme have 80%, 91.72% and 95.11%. It shows that our scheme gives better PDR than the above schemes.

Simulation results of proposed and the existing schemes are depicted in Fig. 9 using end-to-end delay metric. Our scheme takes only 88.14 while CLS[32] scheme takes 89.15 ms, SAODV[22] takes 102.46 ms and standard AODV[4] takes 171.46 ms, when the percentage of malicious nodes vulnerable to blackhole attack in networks increases, it is evident that end-to-end delay is substantial. As a result, our scheme has a

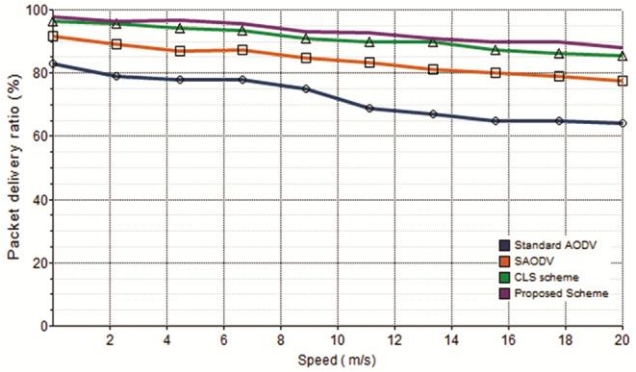

Fig. 8 —Packet delivery ratio (PDR)

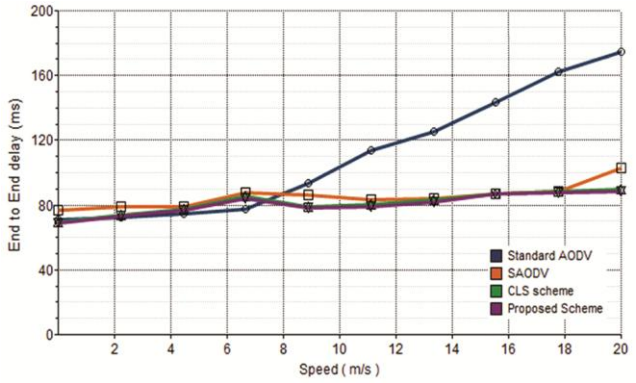

Fig. 9 — Average end-to-end dela

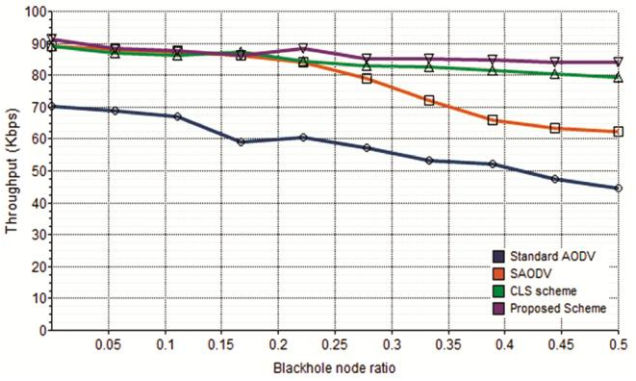

Fig. 10 — Throughput

less end-to-end delay than the previous schemes, which include the standard AODV[4], SAODV[22], and CLS[32] systems.

A comparison graph of throughput between the proposed scheme and existing schemes such as standard AODV, SAODV and CLS scheme, which is depicted in Fig. 10. Here, standard AODV has 70.34 Kbps, SAODV has 89 Kbps, CLS scheme has 89.15 Kbps while proposed scheme has 91.36 Kbps using throughput as a performance metric. Hence our scheme is better than three schemes such as standard AODV, SAODV and CLS scheme.

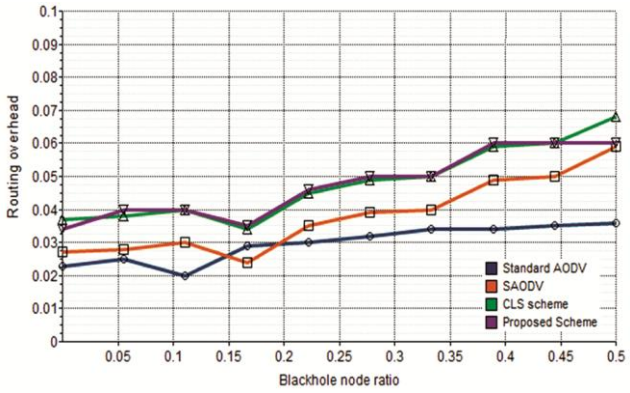

Fig. 11 — Routing overhead

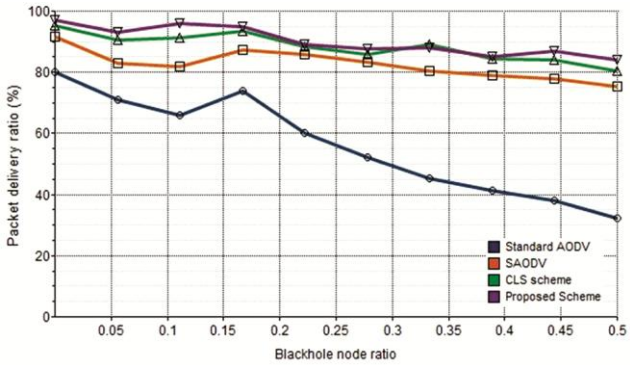

Fig. 12 — Packet delivery ratio

It is observed that our scheme takes least routing overhead as compared to CLS scheme as shown in Fig. 11. Simulation results show that our scheme has 0.034 while standard AODV, SAODV and CLS scheme have 0.2, 0.024 and 0.037. It shows that our scheme is better than CLS scheme.

Scenario 2: Effect on performance metrics when we are varying mobility with fixed % of malicious nodes under blackhole attack:

The response of PDR to increase in network node mobility is illustrated in Fig. 12. According to the results of our simulation, the proposed scheme has a higher PDR than the AODV, SAODV, and CLS schemes. With a constant fraction of malicious nodes, PDR is seen to decline as mobile node mobility increases. Our scheme has 97.93% while standard AODV, SAODV and CLS scheme having 83%, 91.72% and 96.28%. It shows that our scheme outperforms other three schemes.

Simulation results of proposed and the existing schemes using end-to-end performance metric is depicted in Fig. 13. From the results, it shows that standard AODV takes 174.46 ms, CLS scheme takes 89.72 ms and SAODV has 102.56 ms while our

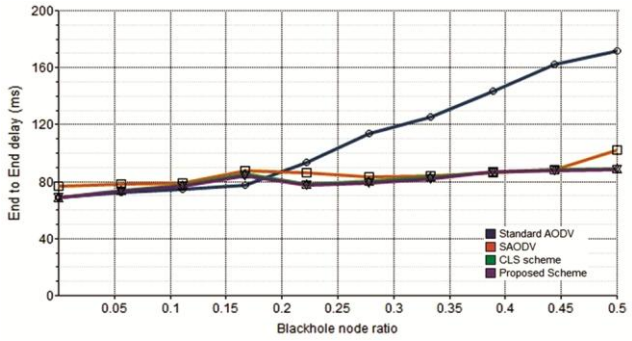

Fig. 13 — End to end delay

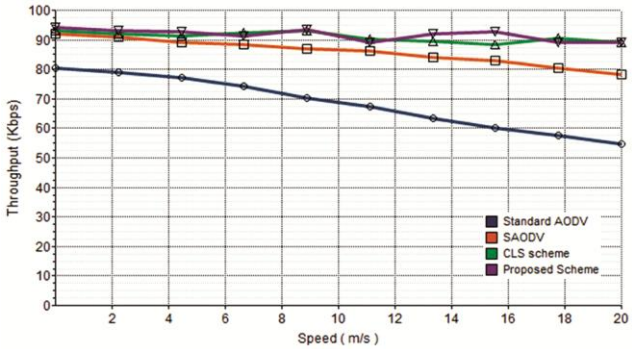

Fig. 14 —Throughput

scheme has only 88.24 ms when we are varying mobility of nodes. It shows end-to-end delay increases when we are varying mobility with fixed number of percentages of malicious nodes in the networks. Hence, our scheme outperforms the other three schemes.

Simulation results between the existing schemes and proposed scheme using throughput as a performance metric is shown in Fig. 14. Here, standard AODV has 80.34 Kbps, SAODV has 92 Kbps, and CLS scheme has 93.15 while proposed scheme has 94.30 Kbps. Hence our scheme outperforms other three schemes such as standard AODV, SAODV and CLS scheme.

CLS scheme exhibits the highest routing overhead as compared to other schemes, which is represented in Fig. 15. It is observed that our scheme produces least routing overhead as compared to SAODV and CLS scheme. Simulation results show that our scheme has 0.046 while standard AODV, SAODV and CLS schemes have 0.034, 0.052 and 0.057.

Complexity Analysis: This Section contains the time complexity of our method and other existing methods. Here we use some notations in complexity analysis are as follows:

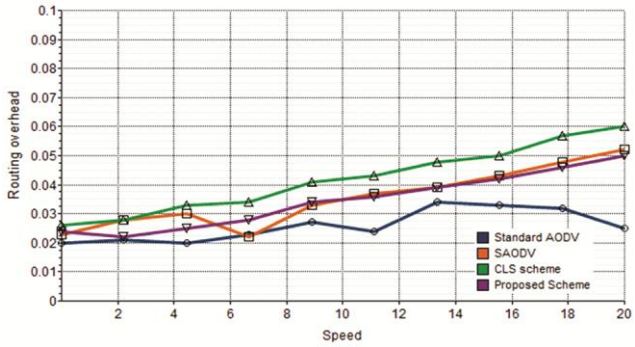

Fig. 15 — Routing overhead

Table 4 — Time Complexity

Zhang *et al.*[33]	$3T_{SM} + 8T_E + 4\ T_s + 7\ T_H$
Sharma *et al.*[34]	$5T_{SM} + 8\ T_E + 2\ T_s + 7\ T_H$
Our scheme	$6T_{SM} + 7T_E + 2T_s + 7T_H$

Table 5 — Comparison of basic security requirements

S.N.	Parameters Protocols	AODV[4]	SAODV[22]	Our Scheme
1.	Authentication	X	✔	✔
2.	Integrity	X	✔	✔
3.	Secrecy	X	X	✔
4.	Non-repudiation	X	✔	✔
5.	Forward Secrecy	X	X	✔
6.	Backward Secrecy	X	X	✔
7.	Group Key Secrecy	X	X	✔

TSM: Time for Scalar Multiplication
TE: Time for Exponential Operations
TA: Time for Addition Operations
TS: Time for Subtraction Operations
TH: Time for Hash Function

Proposed scheme takes less exponential operations i.e. T_E with respect to above two schemes, which is shown in Table 4.

Comparison of security goals: Our scheme provides important security goals such as integrity, non-repudiation and authentication. Table 5 shows a comparison between existing schemes and proposed scheme in terms of important security goals.

Conclusions

In this paper, we proposed an RSA signature scheme for prevention of malicious nodes i.e. blackhole attack in MANET. It also provides a secure data communication between a sender and receiver end. We have considered two scenarios: Scenario 1: affects performance metrics when we vary the number of malicious nodes without changing mobility while the second situation affects performance metrics with varying mobility of the nodes in the presence of fixed

malicious nodes. Our simulation findings for scenario 1 show that the proposed system outperforms traditional schemes AODV, SAODV and CLS in terms said performance metrics. In Scenario 2, our scheme has better results as said performance metrics. It is observed that our scheme successfully prevented from blackhole attack.

The scope of this paper is to provide security against blackhole attack in MANET using RSA based certificateless signature scheme. Performance evaluation of proposed scheme has been carried out under network simulator (ns-2). From the simulation results, it is more efficient in terms PDR, throughput, routing overhead and end-to-end delay when we are varying mobility and fixed percentage of malicious nodes. It also provides important security services viz., integrity, authentication and non-repudiation. Proposed scheme is capable to prevent single blackhole attack and are unable to prevent form cooperative blackhole attack in MANET. As future work, we intend to apply our scheme in various emerging areas such as FANET, VANET, cloud computing, and secure mail system, grid computing and electronic commerce.

References

1 Abel Vikas S, Survey of attacks on mobile adhoc wireless networks, *Int J Comput Sci*, **3** (2011) 826–829.

2 Saha S, Chaki R & Chaki N, A new reactive secure routing protocol for mobile ad-hoc networks, *Proc Comput Info Sys & Indus Manag Appl*, **84** (2008) 103–108.

3 Nadeem A & Howarth M P, A survey of MANET intrusion detection & prevention approaches for network layer attacks, *IEEE Commun Surv*, **15** (2013) 2027–2045.

4 Perkins C E, Ad hoc networking: An introduction, *Ad Hoc Netw*, **40** (2001) 20–22.

5 Kumar S & Dutta K, Security issues in mobile ad-hoc networks: A survey in *Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications*, (IGI Global, USA) 2014, 176–221.

6 Wu B, Chen J, Wu J & Cardei M, A survey of attacks and countermeasures in mobile ad hoc networks in *Wirel Netw*, (Signals and Communication Technology, Springer, Boston, USA) 2007, 103–135.

7 Biswas K & Ali M, *Security Threats in Mobile Ad Hoc Network*, Master Thesis, Blekinge Institute of Technology, Sweden, 2007.

8 Rai A K, Tewari R R & Upadhyay S K, Different types of attacks on integrated manet-internet communication, *Int J Comput Sci & Sec*, **4** (2010) 265–274.

9 Djenouri D, Khelladi L & Badache N, A survey of security issues in mobile ad hoc networks, *IEEE Commun Surv*, **4** (2005) 2–28.

10 Goyal P, Batra S & Singh A, A literature review of security attack in mobile ad-hoc networks, *Int J Comput Appl*, **12** (2010) 11–15.

11 She C, Yi P, Wang J & Yang H, Intrusion detection for black hole and gray hole in MANETs, *KSII Trans Internet Inf Syst*, **7** (2013) 1721–1736.

12 Kannhavong B, Nakayama H, Nemoto Y, Kato N & Jamalipour A, A survey of routing attacks in mobile ad hoc networks, *IEEE Wirel Commun*, **5** (2007) 85–91.

13 Khanna A & Dere P U, A Review on intrusion detection and security of wormhole attacks in MANET, *Int J Sci Res*, **12** (2014) 873–876.

14 Kumar V & Kumar R, An adaptive approach for detection of blackhole attack in mobile ad hoc network, *Procedia Comput Sci*, **48** (2015) 472–479.

15 Kumar V & Kumar R, A cooperative black hole node detection and mitigation approach for MANETs, *Lect Notes Comput Sci*, 2015 171–183.

16 Tseng F, Chou Li & Chao H, A survey of black hole attacks in wireless mobile ad hoc networks, *Hum-centric Comput Inf Sci*, **1** (2011) 1–16.

17 Ullah I & Rehman S U, *Analysis of Black Hole Attack on Manets using Different MANET Routing Protocols*, Master Thesis, Blekinge Institute of Technology, Sweden, 2010.

18 Zhang X, Sekiya Y & Wakahara Y, Proposal of a method to detect black hole attack in MANET, *Proc Int Sympo Auton Decent Sys*, (Athens, Greece) 2009, 1–6.

19 Sowmya K S, Rakesh T & Hudedagaddi D P, Detection and prevention of blackhole attack in MANET using ACO, *Int J Comput Netw Secur*, **12** (2012) 21–24.

20 Tamilselvan L & Sankaranarayanan V, Prevention of co-operative black hole attack in MANET, *J Netw*, **3** (2008) 13–20.

21 Panda G, Mishra G S & Sahoo A K, Prevention of black hole attack in AODV protocols for Mobile Ad Hoc network by key authentication, *Int J Comput Sci Inf Technol*, **2** (2012) 651–657.

22 Zapata M G, Secure ad hoc on-demand distance vector routing, *Mob Comput Commun Rev*, **6** (2002) 106–107.

23 Raj P N & Swadas P B, Dpraodv: A dyanamic learning system against blackhole attack in AODV based MANET, *Int Comput Sci I*, **2** (2009) 54–59.

24 Hu Y C, Perrig A & Johnson D B, Ariadne: A secure on-demand routing protocol for ad hoc networks, *Wirel Netw*, **11** (2005) 21–38.

25 Kurosawa S, Nakayama H, Kato N, Jamalipour A & Nemoto Y, Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method, *Int J Netw Secur*, **5** (2007) 338–346.

26 Deng H, Li W & Agrawal D P, Routing security in wireless ad hoc networks, *IEEE Commun Mag*, **40** (2002) 70–75.

27 Ghosh T, Pissinou N & Makki K, Collaborative trust-based secure routing against colluding malicious nodes in multi-hop ad hoc networks, *Proc L Comput Netw*, (Tampa, Florida, U.S.A.) 2004, 224–231.

28 Gajera M & Sowmya K S, Prevention of black hole attack in secure routing protocol, *Int J Sci Res*, **2** (2013) 221–224.

29 Jaiswal P & Kumar R, Prevention of black hole attack in MANET, *Int J Comput Netw Commun*, **2** (2012) 599–606.

30 Maheshwar K & Singh D, Black hole effect analysis and prevention through IDS in MANET environment, *Eur J Sci Res*, **1** (2012) 84–90.

31 Singh H & Singh M, Securing MANETs Routing Protocol under Black Hole Attack, *Int J Innov RES Comput Commun Eng*, **1** (2013) 808–813.

32 Kumar V & Kumar R, *Security Solutions for Hyperconnectivity and the Internet of Things: Prevention of blackhole attack using certificateless signature (CLS) scheme in MANET* (IGI Global) 2017, 130–150.

33 Zhang J & Mao J, An efficient RSA-based certificateless signature scheme, *J Syst Softw*, **85** (2012) 638–642.

34 Sharma G & Verma A K, Breaking the RSA-based certificateless signature scheme, *Information*, **16** (2013) 7831–7836.

35 Zeadally S, Hunt R, Chen Y S, Irwin A & Hassan A, Vehicular ad hoc networks (VANETS): status, results, and challenges, *Telecommun Syst*, **50** (2010) 217–241.

36 Samara G, Al-Salihy W A & Sures R, Security analysis of vehicular Ad Hoc networks, *Proc Netw Appli Protoc Serv* (Alor Setar, Kedah, Malaysia) 2010, 55–60.

37 Bekmezci I, Sahingoz O K & Temel Ş, Flying ad-hoc networks (FANETs): A survey, *Ad Hoc Netw*, **11** (2013) 1254–1270.

38 Gurung S & Chauhan S, A dynamic threshold based approach for mitigating black-hole attack in MANET, *Wirel Netw*, **24** (2018) 2957–2971.

39 Gupta P, Goel P, Varshney P & Tyagi N, Reliability factor based AODV protocol: Prevention of black hole attack in MANET, *Proc S Innovat Commun & Comput Sci* (Vaigai College Engineering, Madurai, India) **851** (2018) 271–279.

40 Gurung S & Chauhan S, A survey of black-hole attack mitigation techniques in MANET: merits, drawbacks, and suitability, *Wirel Netw*, **26** (2019) 1981–2011.

41 Rani P, Verma S & Nguyen G N, Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network, *IEEE Access*, **8** (2020) 121755–121764.

42 Karthigha M, Latha L & Sripriyan K, A comprehensive survey of routing attacks in wireless mobile ad hoc networks, *Proc Invent Comput Tech* (Coimbatore, India) 2020, 396–402.

43 Shukla M, Joshi B K & Singh U, Mitigate wormhole attack and blackhole attack using elliptic curve cryptography in MANET, *Wirel Pers Commun*, **121** (2021) 503–526.

44 Hussain K, Abdullah A H, Iqbal S, Awan K M & Ahsan F, Efficient cluster head selection algorithm for MANET, *J Comput Netw Commun* (2013).