Human-centric Computing and Information Sciences
a SpringerOpen Journal

REVIEW Open Access

# An effective implementation of security based algorithmic approach in mobile adhoc networks

Rajinder Singh[1*], Parvinder Singh[2] and Manoj Duhan[3]

* Correspondence:
rajpanihar@rediffmail.com
[1]Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Haryana, India
Full list of author information is available at the end of the article

**Abstract**

Mobile Ad-hoc Network one of the prominent area for the researchers and practitioners in assorted domains including security, routing, addressing and many others. A Mobile Ad-hoc Network (MANET) refers to an autonomous group or cluster of mobile users that communicate over relatively bandwidth constrained wireless links. Mobile ad hoc network refers to the moving node rather than any fixed infrastructure, act as a mobile router. These mobile routers are responsible for the network mobility. The history of mobile network begin after the invention of 802.11 or WiFi they are mostly used for connecting among themselves and for connecting to the internet via any fixed infrastructure. Vehicles like car, buses and trains equipped with router acts as nested Mobile Ad-hoc Network. Vehicles today consists many embedded devices like build in routers, electronic devices like Sensors PDAs build in GPS, providing internet connection to it gives, information and infotainment to the users. These advances in MANET helps the vehicle to communicate with each other, at the time of emergency like accident, or during climatic changes like snow fall, and at the time of road block, this information will be informed to the nearby vehicles. Now days technologies rising to provide efficiency to MANET users like providing enough storage space, as we all know the cloud computing is the next generation computing paradigm many researches are conducting experiments on Mobile Ad-hoc Network to provide the cloud service securely. This paper attempts to propose and implement the security based algorithmic approach in the mobile adhoc networks.

**Keywords:** MANET; Network security; Wormhole attack; Secured algorithm

## Introduction

Now days, lots of research is going on in the domain of mobile ad hoc networks. One of the major issues in the mobile ad hoc networks is the performance - in a dynamically varying topology; the nodes are expected to be power-aware because of the bandwidth constrained network. Another matter in such networks is security - as each node participates in the operation of the network equally, malicious nodes are intricate to identify. There are several applications of mobile ad hoc networks such as disaster management, ware field communications, etc. To analyze and detailed investigation of these issues, the scenario based simulation of secure protocol is done and compared with classical approaches. The scenarios used for the simulation and predictions depict critical real-world applications including battlefield and rescue operations but these can be used in many other applications also.

In ad hoc networks all nodes are responsible of running the network services meaning that every node also works as a router to forward the networks packets to their destination. It is very challenging for researchers to provide comprehensive security for ad hoc networks with the desired quality of service from all possible threats. Providing security becomes even more challenging when the participating nodes are mostly less powerful mobile devices.

Wireless Ad Hoc networks have been an interesting area of research for more than a decade now. What makes ad hoc networks interesting and challenging is its potential use in situations where the infrastructure support to run a normal network does not exist. Some applications include a war zone, an isolated remote area, a disaster zone like earthquake affected area and virtual class room etc.

In ad hoc networks all nodes are responsible of running the network services meaning that every node also works as a router to forward the networks packets to their destination. It is very challenging for researchers to provide comprehensive security for ad hoc networks with the desired quality of service from all possible threats. Providing security becomes even more challenging when the participating nodes are mostly less powerful mobile devices. In this paper an effort has been made to evaluate various security designs proposed.

## Security aspects in mobile ad hoc networks

In any classical fixed or wireless network, the security is implemented at three stages: prevention, detection and cure. The key parts of prevention stage include authentication and authorization. The authentication is concerned with authenticating the participating node, message and any other meta-data like topology state, hop counts etc. Authorization is associated with recognition. The point where detection is the ability to notice misbehavior carried out by a node in the network, the ability to take a corrective action after noticing misbehavior by a node is termed as cure.

Assorted possible attacks that are implemented on ad hoc networks are eavesdropping, compromising node, distorting message, replaying message, failing to forward message, jamming signals etc. The central issues behind many of the possible attacks at any level of security stage are authentication, confidentiality, integrity, non repudiation, trustworthiness and availability.

## Assumption and dependencies

- Basically Ad-hoc Networks depends upon any fixed infrastructure or any other mobile node to communicate, through forwarding and receiving packets.
- Comparing the security issues of wireless ad-hoc network with wired ad-hoc network, wired network has the proper infrastructure for forward and receiving packets, whereas in wireless network there is no proper infrastructure and it is accessible by both authorized users and hackers.
- In this wireless ad-hoc network there is no particular design to monitor the traffic and accessibility, these leads to third party intervention like malicious users.

In this manuscript, various issues are focused that affect the ad-hoc networks security mechanism and also to concentrate on pros and cons of Mobile networks protocols.

The focus on enhancing security and reliability to Mobile Ad-hoc Network (MANET) [1] is also addressed.

Many researches were done before to provide security to MANET [1] but none of the protocol shines in providing security and performance. There are many defects in the Mobile framework; this may cause unknown nodes to connect frequently without any proper routing. In order to prevent other nodes from trespassing we are going to concentrate on providing more security to Mobile Ad-hoc network.

There were so many research areas in MANET [1] in that security is the major concern among others.

The scope of securing MANET [1] is mentioned here

- Securing MANETs [1] is great challenge for many years due to the absence of proper infrastructure and its open type of network.
- Previous security measures in MANETs [1] are not effective in the challenging world with advancement in technology.
- Many layers often prone to attacks man in middle attack or multilayer attack, so proposal should concentrate on this layers.
- The proper intelligent approach [2] of securing MANETs [1] has not yet discovered.
- In this project we are going to concentrate on applying bio inspired intelligence [2] techniques for securing MANETs.

## Problem identification

- The main objective of the manuscript is providing security to the existing systems mainly on the network layer to prevent the attacks like wormhole attacks [3] etc.
- To analyze the scope of multi layer attacks [4].
- To evaluate the techniques like Genetic Algorithms [5], Swarm Intelligence [6], Memetic Algorithms [7] etc.
- To analyze the needs of above mentioned techniques in different network layers especially in the multi link layer.
- To propose a unique technique for above mentioned attacks.
- Intelligent MANET [6] proposal to deal with all kinds of attacks.
- To validate the above techniques by implementing and analyzing its results with the existing systems.

## Applications

- It provides a relative study of the systems under the parameters packet loss, packet delivery rate and network connectivity.
- A better understanding of the Quality of Service (QoS) parameters can be obtained and they can be used for solving various networking complexities.

## Hardware requirements

The minimum requirements needed to perform operations are

- Intel Pentium Processor at 2 GHz or Higher

- RAM 256 MB or more
- Hard disk capacity 10 GB or more

## Software requirements

The software required to perform the implementation are

- Linux Operating System (Ubuntu, Fedora)
- NS2, NAM tools
- GNU Plot

## Manet security attacks

Malicious node [8] is one which causes attacks on various layers on MANET like application layer, data link layer, physical and network layer.

There were two types of attacks on MANET, they are

- Active attacks
- Passive attacks

## Active attacks

In this attack, some harmful information is injected into the network, which causes malfunctioning of the other nodes or network operation. For performing this harmful information it consumes some sort of energy from other nodes, those nodes are called as malicious node.

### Passive attacks

In this passive attack, the malicious nodes disobey to perform its task for some sort reasons like saving energy for its own use of moving randomly, by diminishing the performance of the network.

### Network layer attack

Let us concentrate on various attacks on the network layer.

### Wormhole attack

Wormhole attack [3] is also known as tunnelling attack, in this tunnelling attack the colluding attackers build tunnel between the two nodes for forwarding packets claiming that providing shortest path between the nodes and taking the full control of the nodes, which is invisible at the higher layers.

Figure 1 represents the wormhole attack, where S and D nodes are the source and destination, A B and C are the connecting nodes providing path between source and destination. M and N are the malicious nodes, tunnelled by colluding attackers.

## Existing technique for preventing wormhole attack

In the previous techniques wormhole attack is prevented using the Location based Geo and Forwarding (LGF) Routing Protocol.

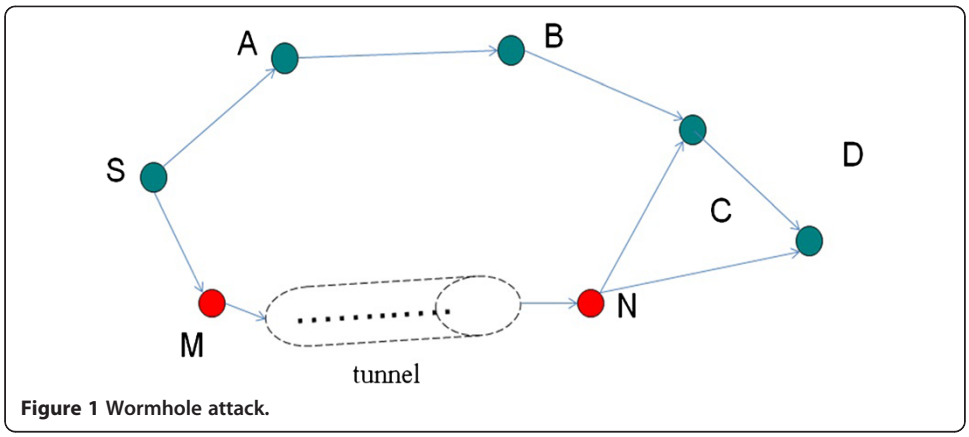


**Figure 1** Wormhole attack.

## Implementation of lgf routing protocol

There are several steps in implementing LGF routing protocol, consider source node S wants to communicate with destination node D (Figure 2).

- The Source node multicast the RREQ message to all the intermediate which contains the IP address of the destination node based on distance of the destination node.
- This protocol is tested with source node 100 M away from the destination node and the intermediate nodes as
  DIST (S, 1) = 40 M
  DIST (S, 2) = 53 M
  DIST (S, 5) = 48 M
  DIST (1, 3) = 60 M

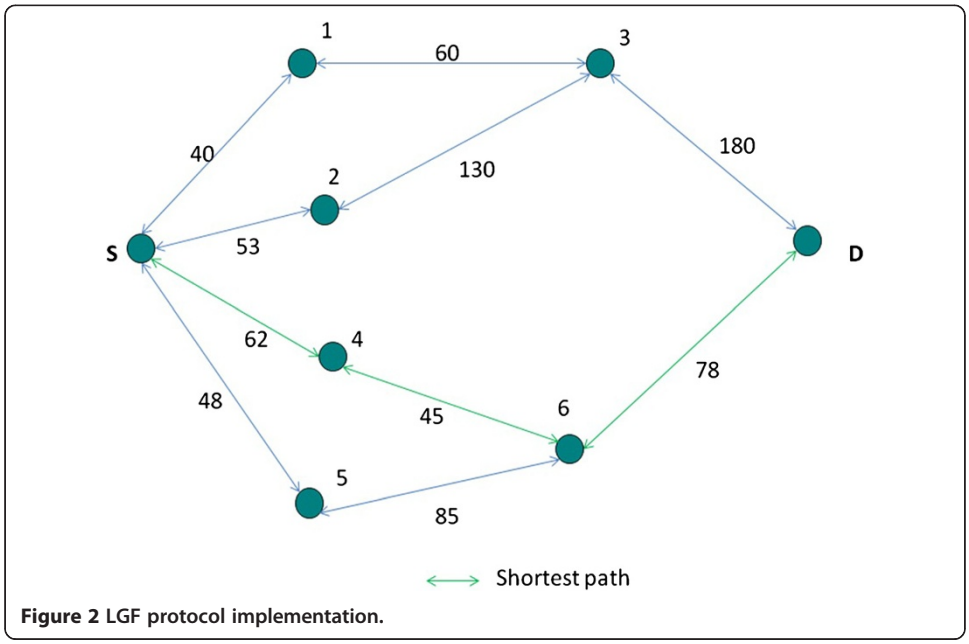


**Figure 2** LGF protocol implementation.

DIST (2, 3) = 130 M
DIST (3, D) = 180 M
DIST (4, 6) = 45 M
DIST (S, 4) = 62 M
DIST (5, 6) = 85 M
DIST (6, D) = 78 M

- Compare distance between source and destination using the following code
  If (intermediate nodes < source node S to destination node D distance)
  {
  These are the nodes in between S to D, can conditionally transfer the RREQ packet to D.
  }
  Else
  {
  The intermediate node is out of transmission area, so send RREQ error message to S node
  }
- RREQ has been received in destination node, start D node sending RREP packet towards the intermediate node to reach the source node.
- S node received RREP packet from different intermediate nodes, compare the distance from different intermediate nodes.
- Select the shortest path between the source and destination node with respect to the received RREP packet and then send the original packets between S and D node this was the technique used in LGF protocol.

However the preventive measures of wormhole attack with this LGF protocol was not solved clearly.

## Black hole attack

Black hole attack [8] is the serious problem for the MANETs, in this problem a routing protocol has been used by malicious node reports itself stating that it will provides shortest path.

In flooding based protocol, a fake route is created by the malicious node rather than the actual node, which results in loss of packets as well as denial of service (DoS).

In the Figure 3, S and D nodes are the source and destination nodes, A B C are the intermediate nodes and M is the malicious node. RREQ and RREP are the key terms for route request and route reply respectively. MREP is abbreviation for malicious reply.

## Existing technique

### Two tier secure AODV (TTSAODV)

TTSAODV protocol is proposed earlier to prevent the black hole attack. In these protocol two levels of security is provided

1. During route discovery mechanism and
2. During data transfer mechanism

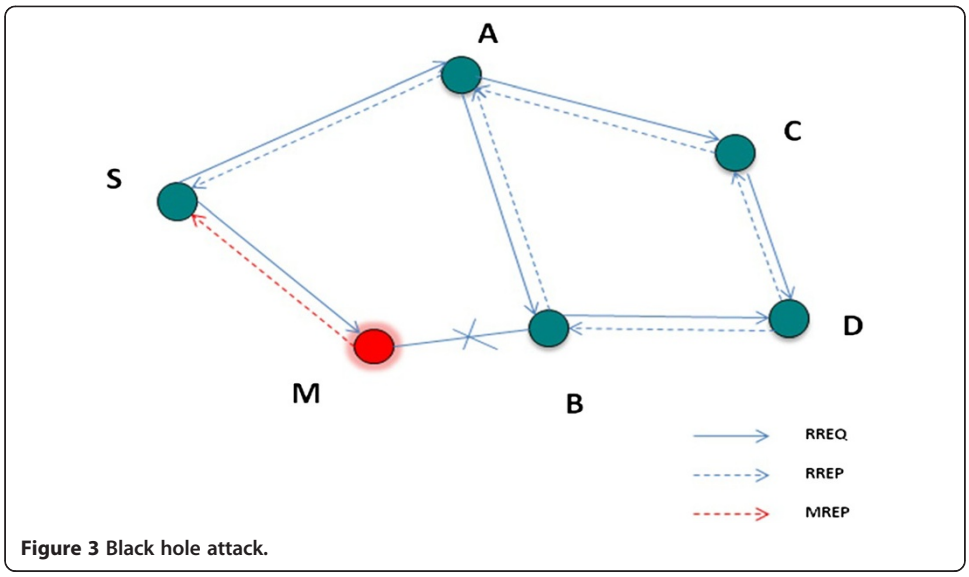


**Figure 3** Black hole attack.

In this technique, black hole attack is easily identified either of these two techniques, even it fails in any of the mechanism. The major drawback in this technique causes enormous packet loss and delay in transferring packet.

### Resource consumption attack

In the resource consumption attack, a malicious node can try to consume more battery life demanding too much of route discovery, or by passing unwanted packets to the source node.

### Location disclosure attack

In the location disclosure based attack, the malicious node collects the information of routes map and then focus on further attacks. This is one of the unsolved security attacks against MANETs.

### Multi layer attacks in manet

There are different types of multilayer attacks in MANET, they are as follows

- Denial of Service (DoS)
- Jamming
- SYN flooding
- Man In Middle attacks
- Impersonation attacks

### Alpha numeric based secure reflex routing

In this, proposed algorithm prevents the worm-hole attacks by routing the data through the authorized nodes like LN, and AN nodes through this way the communication takes place.

In the proposed algorithm the worm-hole tunnel is prevented through the following steps (Figure 4).

### Step 1

Since every connection through nodes is possible only through Leader Node and Access node so there is impossible for a malicious node to make tunnel from the source node.

### Step 2

The Leader Node manages the routing table and also the details of all the nodes in its group, it also contains the details of whether the particular node is Access Node or normal node. The Leader node also maintains details about other groups Leader Node and its address with the help of its Access Nodes.

### Step 3

The normal node in a group maintains a table that contains information of its Leader Node address and the common identifier generated by the Leader Node. The Access nodes have a table that maintains the other Leader Nodes common identifiers.

### Step 4

The address of the Leader Node that has already involved in routing has stored in every packet, it is used for verification by other Leader Nodes.

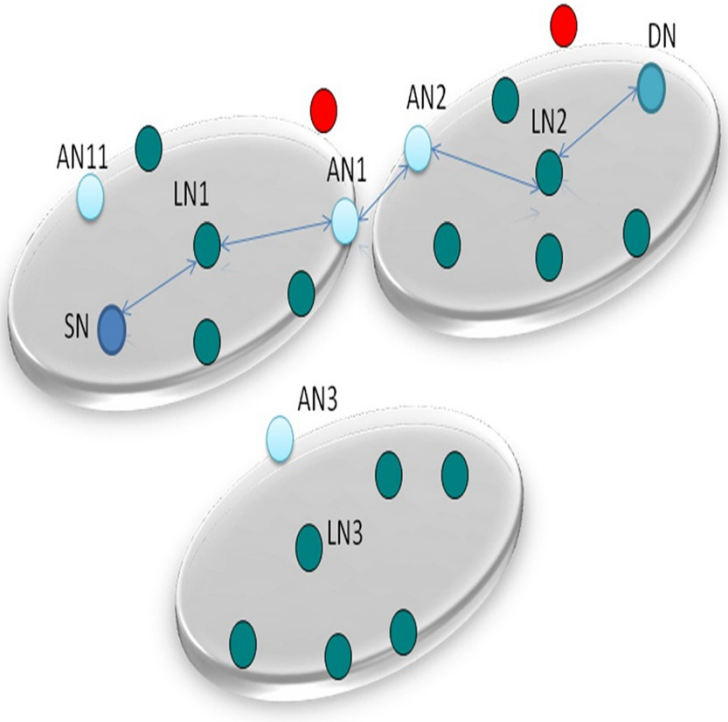


**Figure 4** Proposed Worm-hole prevention technique.

#### Step 5

When a source node in a need of route to deliver packets to the destination node, it sends Route Request message to the Leader node, the Leader Node uses its common identifier to verify the packet with alpha numeric values.

#### Step 6

The leader Node checks whether the destination node is in house, if the destination node is present under the leader node, then it sends the packet directly. If the destination node is not in house then it sends Route Request message to all its Access nodes, The Access nodes using their common identifier verifies the alpha numeric values from Leader node then transfers that packet to the neighbours Access Node.

#### Step 7

The neighbour Access node checks whether the packet came from its neighbour Leaders node or from any malicious node by common identifier that has previously exchanged, then it sends the Route Request message to its Leader Node, this Leader Node verifies the Leader node details and include its details in that packet and forwards the original packet until it reaches the destination.

#### Step 8

Finally the destination node checks whether the packet came from its Leader node or from any malicious node using the identifier, after verification process is over it accepts the packet.

#### Step 9

Destination node sends the Reply Request message (RREP) to source node through the same route already followed for transferring packet.

#### Step 10

In case the any node involved in the routing moves away from one group into the another group, the previous process is not needed as it is already registered in that network, some other node in that group replace the previous node.

#### Step 11

Suppose if the source node or destination node moves away from its group, the foreign Access Node acts as a relay node for forwarding packets this process minimizes the time for authenticating in newer group.

## Proposed architecture

### Worm-hole attack prevention using alpha numeric reflex routing algorithm

In this technique, there won't be any possibilities for a malicious node to make tunnelling between the source and the destination nodes, as it is not included in the either of any groups. The packets are safe to reach the destination node efficiently.

**Pseudocode for alpha numeric reflex routing algorithm**

BEGIN

Initialize nodes

Initialize source and destination nodes

FOR $i = 0\ to\ n$ DO

$LN_i \leftarrow$ Nodes with higher battery power, ability to manage other nodes

IF (nodes in range of $LN$) THEN

$Transmit\ common\ identifier$

ELSE

The node is under other $LN$

END IF

END FOR

FOR $i = 0\ to\ n$ DO

FOR $j = j + 1\ to\ n$ DO

$AN_{ij} \leftarrow$ Nodes receive *common identifier* from other $LN$

IF (*node* accepts the *common identifier* and replies its details to *LN*) THEN

$Node = trusted$

ELSE

$Node = malicious$

END IF

$Source\ node \rightarrow Forward\ RREQ$

IF (*source node* and *destination node* is under same *LN)* THEN

$Forward\ RREQ \rightarrow destination\ node$

ELSE

$Forward\ RREQ \rightarrow AN_{ij}$

$AN_{ij} \rightarrow LN_i$

$LN_i \rightarrow destination\ node$

END IF

END FOR

END FOR

END

**Proposed algorithm to prevent black hole attack**

In this proposed algorithm, the Expected broadcast count algorithm is introduced. With the help of this algorithm highest throughput is possible between the nodes but however the actual algorithm does not prevent the black hole attack.

Throughput refers to the average number of message transmitted in a given time, it is usually measured in bps or bits per second, and it is also mentioned as packet delivery ratio. Malicious node plays a major role in affecting throughput in black hole attacks.

Secure mesh network measurement technique is proposed in this project to prevent the black hole attacks during route discovery process between the source and destination node with the help of the throughput measurement values, this makes the routing process more consistent and efficient communication between the nodes.

#### Expected broadcast count algorithm

This *EBX* algorithm is used to increase throughput in MANETs, it is referred as the expected number of packets transmission and retransmission required to successfully deliver a packet in the network.

It is calculated using the delivery ratio of packets in destination node $d_d$ and delivery ratio of packets in the source node $d_s$, $d_d$ is the prospect of forward packet transmission and $d_s$ is the reverse packet transmission.

These $d_s$ and $d_d$ values are calculated from the acknowledgement packets known as query, nodes commonly exchanges their query message with their neighbours after delivering each packet.

Suppose consider a link from $A \rightarrow B$ where $A$ and $B$ are the nodes, these two nodes determined themselves to send query message for particular time gap period $g/\tau$, where as $\tau$ = jitter (packet delay variations).

$A$ and $B$ counts the number of query they received from each other during gap period *count* $(t-g,t)$ then $A$ calculates the $d_d$ from the equation.

$$d_d = count(t-g,t)/\left(\frac{g}{t}\right) \tag{1}$$

Where *count* $(t-g,\ t)$ is the number of query commenced by node $B$ and received by node $A$.

The node $B$ calculates the $d_s$ in similar way to $d_d$.

$$d_s = count(t-g,t)/\left(\frac{g}{t}\right) \tag{2}$$

$A$ and $B$ swaps the $d_s$ and $d_d$ values to calculate the EBX.

$$EBX_{A\rightarrow B} = \frac{1}{d_{s*}d_d} \tag{3}$$

This equation is used to find *EBX* value for more routes, *EBX* value has more hops, and the routes with more number of hops may have lesser throughput due to the intrusion among hops in the same path.

Source and Destination nodes *EBX* value can be calculated through the following formula.

$$EBX_{S\rightarrow D} = EBX_{A\rightarrow B} \tag{4}$$

Less *EBX* value in the routes have fewer possibility of packet loss, and that route is more preferable than others routes (Figure 5, Table 1).

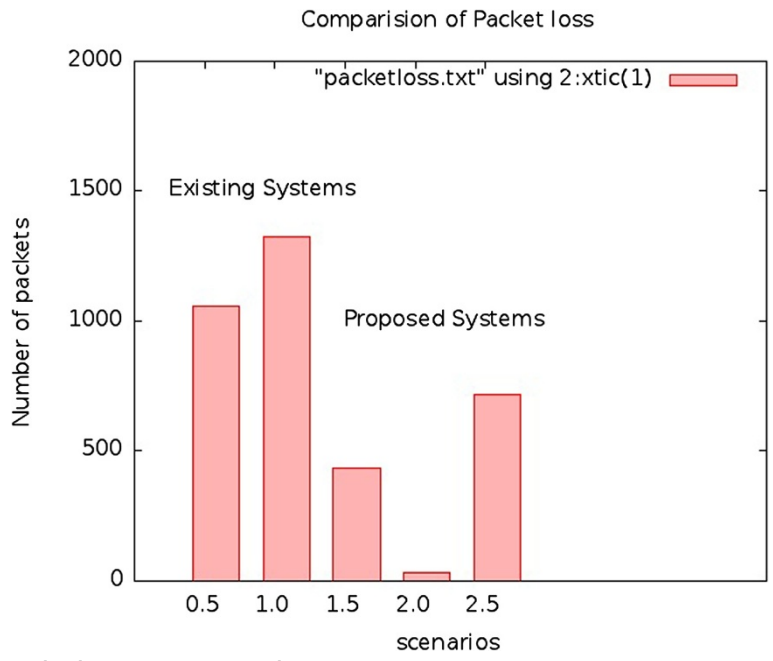


**Figure 5** Packet loss comparison graph.

## Intelligent manet algorithm

In this intelligent approach, nodes connected to this network is monitored by server agent, the server agent manages the details of the mobile nodes in a network like

- Behaviour of the node
- Speed of the node
- Direction of the node
- Position of the node

This technique prevents the malicious node from attacking other nodes (Figure 6).

### Step 1

The nodes participating in the networks to access service like internet registers its identity with the server agent, the server agent replies with unique ID to the requesting node.

### Step 2

The source node request route with the current access point to the destination node the current access point forwards the route request to the server agent.

**Table 1 Packet loss comparisons**

| Scenarios | Time (in seconds) | Packet drop (in bits) |
|---|---|---|
| Existing system 1 | 6.5 | 10581 |
| Existing system 2 | 6.5 | 13221 |
| Proposed system 1 | 6.5 | 4372 |
| Proposed system 2 | 6.5 | 322 |
| Proposed system 3 | 6.5 | 715 |

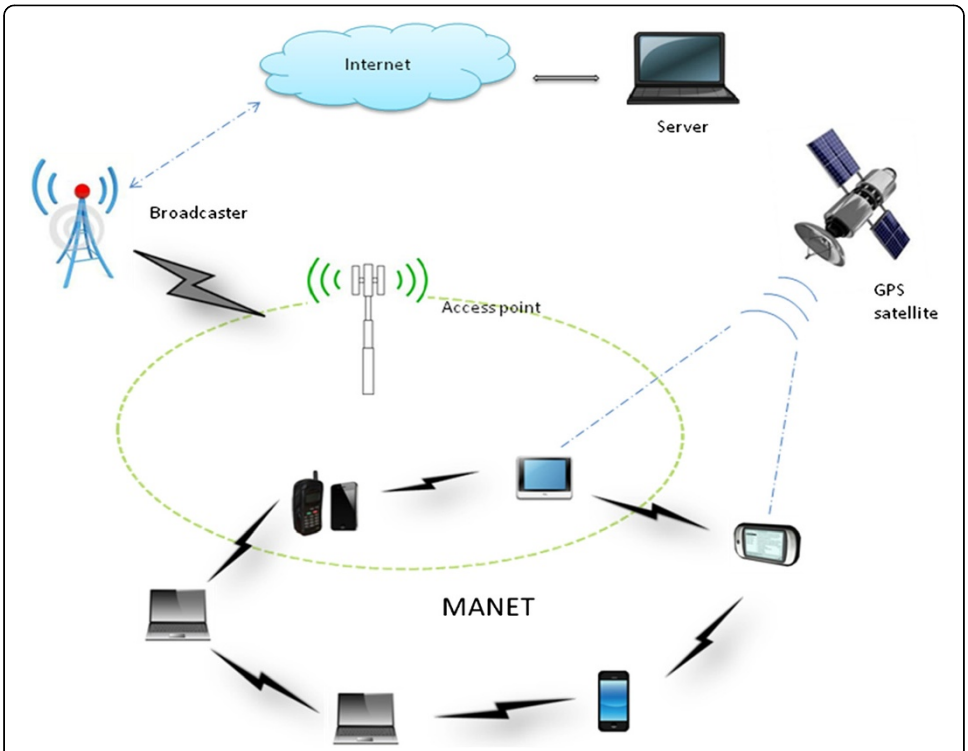


**Figure 6** Intelligent MANET architecture.

### Step 3

The server agent verifies the source ID, then it accepts the route request from sender then it gathers the information of receiver using destination ID from the list.

### Step 4

The server agent then broadcasts the route request message using destination ID, the registered adjacent nodes that are nearer to the destination node which are ready to provide the service replies with the acknowledgement message to the server agent.

### Step 5

The server agent chooses the adjacent node with the longest life time (the ability of the nodes to stay connected with the destination node) using the details collected from the ID, Such as nodes position, direction of motion and speed of the node.

### Step 6

Then the server agent provides route reply message for the source node, after this authentication process, source node starts sending data packets in a secure way.

### Step 7

In case any node moves away from the network, immediately the server agent replaces it with some other nodes to maintain the continuity of connection.

### Step 8

In this technique, the malicious node or selfish nodes are completely eliminated from the network, as the server agent takes full control of the ad-hoc network.

## Conclusion

Mobile adhoc networks are facing vulnerability and security issues from a long time. Assorted protocols and algorithmic approaches has been developed and implemented so far to avoid and remove the issues associated. In this manuscript, we have implemented an empirical and effective approach to optimize the packet loss frequency. The algorithmic approach is implemented in the network simulator ns2 to execute the scenarios and results.

**Competing interests**
The authors declare that they have no competing interests.

**Authors' contributions**
RS carried out the development of algorithmic approach, actual logic and implementation. PS and MD finally analyzed the results. All authors read and approved the final manuscript.

**Author details**
[1]Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Haryana, India. [2]Department of Computer Science and Engineering, Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Haryana, India. [3]Department of Electronics and Communications, Deenbandhu Chhotu Ram University of Science & Technology, Murthal, Haryana, India.

Received: 2 December 2013 Accepted: 9 April 2014
Published online: 19 June 2014

**References**

1. Clausen TH (2007) Introduction to mobile ad-hoc networks, Internet Draft
2. Yu C-F (1989) Security safeguards for intelligent networks. In: IEEE International Conference on World Prosperity Through Communications. ICC '89, BOSTONICC/89. Conference record, vol 3. GTE Lab. Inc, Waltham, MA, USA, pp 1154–1159
3. Choi S, Kim DY, Lee DH, Jung J-i (2008) WAP: wormhole attack prevention algorithm in mobile ad hoc networks, SUTC '08. IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing pp 343–348
4. Li JH, Das S, McAuley A, Lee J, Stuhrmann T, Gerla M (2010) A multi-layer approach for seamless soft handoff in mobile ad hoc networks. Hui Zeng Intell. Autom., Inc. (IAI), Rockville, MD, USA, pp 21–26, GLOBECOM Workshops (GC Wkshps), IEEE
5. Leonard J (1997) Interactive Game Scheduling with Genetic Algorithms, Minor Thesis, RMIT (Royal Melbourne Institute of Technology University). Department of Computer Science
6. Prasad S, Singh YP, Rai CS (2009) Swarm based intelligent routing for MANETs. Int J Recent Trends Eng 1(1)
7. Garg P (2009) "A comparison between memetic algorithm and genetic algorithm for the cryptanalysis of simplified data encryption standard algorithm". Int J Netw Secur Appl (IJNSA) 1(1)
8. Sanjay R, Huirong F, Manohar S, John D, Kendall N (2003) Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks". International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA

doi:10.1186/s13673-014-0007-9
**Cite this article as:** Singh *et al.*: **An effective implementation of security based algorithmic approach in mobile adhoc networks.** *Human-centric Computing and Information Sciences* 2014 **4**:7.