Hindawi Publishing Corporation
Journal of Sensors
Volume 2016, Article ID 5486437, 18 pages
http://dx.doi.org/10.1155/2016/5486437

Research Article

Adaptive Cross-Layer Multipath Routing Protocol for Mobile Ad Hoc Networks

Zeeshan Iqbal,[1] S. Khan,[1] Amjad Mehmood,[1] Jaime Lloret,[2] and Nabil Ali Alrajeh[3]

[1] *Institute of Information Technology, Kohat University of Science and Technology (KUST), Kohat City 26000, Pakistan*
[2] *Integrated Management Coastal Research Institute, Universidad Politecnica de Valencia, Camino de Vera, 46022 Valencia, Spain*
[3] *Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia*

Correspondence should be addressed to Nabil Ali Alrajeh; nabil@ksu.edu.sa

Received 24 March 2016; Accepted 26 May 2016

Academic Editor: Jian Shu

Mobile ad hoc networks (MANETs) are generally created for temporary scenarios. In such scenarios, where nodes are in mobility, efficient routing is a challenging task. In this paper, we propose an adaptive and cross-layer multipath routing protocol for such changing scenarios. Our routing mechanisms operate keeping in view the type of applications. For simple applications, the proposed protocol is inspired from traditional on-demand routing protocols by searching shortest routes from source to destination using default parameters. In case of multimedia applications, the proposed mechanism considers such routes which are capable of providing more data rates having less packet loss ratio. For those applications which need security, the proposed mechanism searches such routes which are more secure in nature as compared to others. Cross-layer methodology is used in proposed routing scheme so as to exchange different parameters across the protocol stack for better decision-making at network layer. Our approach is efficient and fault tolerant in a variety of scenarios that we simulated and tested.

1. Introduction

Mobile ad hoc networks (MANETs) are composed of different nodes being operated in infrastructureless environment. These nodes work in a highly dynamic and random topology [1]. Nodes are distributed and mobile with the capability of self-organizing themselves. MANET nodes have resource constraints such as power, processing, and bandwidth. Comparing with the traditional network, MANET inherits the traditional problems of wired and wireless network. Its basic infrastructure less features imposes another burden on the standardization of network architecture. To compare with that of traditional networks, wireless network security must address two foundation aspects. One is key management, trust establishment, and membership control; the other one deals with network availability and routing security [2].

MANET aim is to think of network where each node is mobile one day without the limitation of nodes. Existing protocol also requires significant changes to cope with the challenges and aims of MANET.

Routing is needed whenever a packet is forwarded from source to destination through some intermediate nodes as in most cases the nodes are not directly connected with each other. Some sort of path finding mechanism is required by protocol, that is, the routing protocol. In case of MANET, routing is a serious research issue as the nodes are mobile in nature. These paths are not always connected; hence, some path maintenance is also an issue. Numerous protocols have been proposed considering the nature and diversity of application. Mostly the routing protocol for MANET falls into three categories, that is, proactive, reactive, and hybrid protocols.

Proactive or table driven routing protocol [3–8] established paths in their routing table before they are required. Nodes operating under proactive protocol continuously propagate routing related information to their neighbors to update their routing table. The exchange of information causes the neighbor nodes to propagate their routing information to compute their own routing tables. This process is periodic in nature. Therefore, a source node before transmitting any data packet gets the full path in advance. In case of any link changes, respective nodes update their routing table by doing the same exchange of information process. The advantage of using proactive approach is quite straightforward; that is, the nodes get the full path in advance. The disadvantage is that nodes are always busy in computing their routing table and network overhead is large. Some of the popular proactive protocols are WRP (Wireless Routing Protocol), DSDV (Destination Sequence Distance Vector), FSR (Fisheye State Routing), and so forth.

Reactive or on-demand routing protocol [9–12] does not maintain routing information. Nodes try to find the routes whenever there is need for data transmission. These protocols do not work in advance. This approach might seem slow, but in reality it is somewhat better than proactive approach, considering the nature of MANET. The nodes are mobile so it is better to find the route at the time of transmission rather than in advance. The main advantage of using reactive protocol is that the overhead is small as no continuous route discovery process is running. However, the disadvantage is the delay because the reactive protocol is searching the path to destination before any transmission. Some of the major routing protocols that fall into the category are AODV (ad hoc on-demand distance vector) and DSR (Dynamic Source Routing), and so forth.

Hybrid routing protocols combine the features of both proactive and reactive routing. Hybrid protocols handle more frequently used paths in a proactive manner, while all other routes in reactive fashion. Some of the hybrid protocols are ZRP (Zone Routing Protocol) [13] and ZHLS (Zone based Hierarchical Link State Routing) [14].

Successful data transmission is a three-step process, that is, route discovery, data transmission, and route maintenance. Before sending any data, packet route request is broadcast to initiate route discovery process. In reply to that, route reply is received. In most of the cases, more than one route reply is received from different routes. Sender chooses one best path among all of them. Normally, this path is the shortest path. Other protocols propose some other way of choosing a single path.

Single path routing may result in congestion affecting the network in terms of bandwidth, throughput and delay. To overcome the problems of single path routing, we are planning to design multipath and cross-layered routing protocol for MANET.

The shortest path problem is that it is normally the central path of the network and normally always congested as every node tries to do data transmission via this central path [15]. Single path protocols are not fault tolerant and do not have the capability to distribute the load. To overcome the disadvantage of single path routing, researchers focus on the idea of multipath routing. It is borrowed from the traditional circuit switched network where call blockages are avoided by diverting call to some other route. Once all paths are known to sender, most important issues are about how to select among all available paths and how to distribute load among nodes.

To cope with the modern day challenges such as application diversity and dynamics changes, establishing path for different application is quite cumbersome. MANET architecture also poses some important limitations, for example, limited bandwidth and energy saving. Researcher tries to find the best path among all available routes to satisfy the need. Evolving from single path to two paths which acts as a backup route in case that primary path fails proves better. This approach also adds the fault tolerant feature where one path breaks while the other one takes over. With the passage of time, these approaches were not sufficient for the user requirement and customer satisfaction. Multipath routing technique was used to achieve more efficiency and load distribution among paths. Multipath approaches are basically divided into two categories, that is, link disjoint and node disjoint multipaths. Shared medium always tends to be congested and also reduces the performance of the network due to packets loss and delay [16]. Multihop communication also needs the mutual cooperation required between physical, MAC, and routing layer. In addition, mobility also poses the need for establishment of new route again and again [17]. Shadowing environment feature RSS (Received Signal Strength) is used for stabilizing the link.

One of the major challenges is also on deciding that how many numbers of paths should be used. Using more paths also adds the excessive overload with very minor improvement in the throughput. Majority approaches used two or three paths for multipath scheme [18–20]. Some of the pros and cons of the multipath routing are provided in Table 1.

Table 1: Multipath routing advantages and disadvantages.

Advantages	Disadvantages
Fault tolerant 3	Longer paths
Load balancing	Special control messages
Bandwidth aggregation	Route request storm
Reduce delay	Inefficient route discover
	Duplicate packet processing

For simulation work, we use AODV (ad hoc on-demand distance vector) [9], DSR (Dynamic Source Routing) [10], OLSR (Optimized Link State Routing) [21], PLQBR (Predictive Location-Based QoS Routing in Ad Hoc Networks) [22], QAODV (Quality of Service for Ad Hoc On-Demand Distance Vector Routing) [23], CEDAR (Core Extraction Distributed Ad Hoc Routing) [24], SAODV (secure ad hoc on-demand distance vector) [25], and CSROR (Cross-Layer Secure and Resource-Aware On-Demand Routing) [26].

AODV [9] works on the philosophy of DSDV by improving the on-demand scheme. This helps in finding the up-to-date routes, also by reducing the route maintenance phase. Only the active nodes will exchange and maintain the control information. Destination sequence number is used by source node to avoid looping and freshness of the route. Like DSR, AODV broadcast RREQ to its neighbors, but unlike DSR source routing is not used. Here, source node and intermediate nodes will store the next hop routing information in its routing table and RREQ will be rebroadcasted. Once the RREQ reaches the final destination, it replies with the RREP to the reverse path where entries are created at the intermediate nodes. In case intermediate nodes know the destination, they will only be allowed to send RREP if their sequence number is equal or greater to the sequence number mentioned in the RREQ. In case any error occurs, RERR (Route ERROR) will be generated and transmitted to both end nodes. RERR also causes the end nodes to remove the corresponding route entries. The main disadvantage of AODV is that if sequence number of source node is very small, then the number is used by intermediate nodes and can lead to stale route too causing the RERR frequently.

DSR [10] is well known to be classified as on-demand routing protocol by saving the bandwidth utilization and power consumption. It is different from others in a sense that it uses source routing by not relying on the routing table information. Source routing also helps in loop free, not requiring up-to-date information, thus saving time. DSR protocol works in two phases, that is, Route Discovery and Route Maintenance, simultaneously. One of the significant differences is no usage of HELLO message. Route discovery phase is carried out by flooding the RREQ (ROUTE REQUEST) in the network. The destination node however on receiving the RREQ replies with the RREP (Route Reply), which follows the same path as RREQ travelled through. Intermediate nodes will rebroadcast the RREQ if the path is not known to them; however, they can reply the source node if they have the fresh path to destination. Route cache is implemented to achieve source routing. In case the destination is not known to intermediate nodes, they will append their address in RREQ and rebroadcast to their neighbor. On the reverse with the help of RREP traversing back through them, intermediate nodes can also update their routing table accordingly too.

OLSR [21] is considered to be the table driven protocol. Nodes will exchange messages with the neighboring nodes in the network on regular time interval to update topological information about the network. MPR (Multipoint Relay) is used as a key role to reduce the flooding of the classical mechanism. HELLO messages will be transmitted by nodes to gain knowledge about their one hop neighbor. MPR are the subset of node among one hop neighbors which will be used to forward broadcast information rather than every node retransmitting message whenever it is received for the first time. Link state information is also generated by these MPR nodes only, thus also reducing the control messages flooding. MPR also helps nodes in finding the optimal routes and works well for large and dense network.

PLBQR [22] proposes a mechanism where nodes future physical location is predicted depending on its previous location updates, which in turn to predict the future routes. Stale routes are avoided by prediction the future location of nodes, thus increasing path reliability in terms of location. QoS routing used the update protocol, location, and delay prediction mechanisms. In update protocol, each node will broadcast its geographical update and resource information periodically and in case of major movement, respectively, called Type 1 update and Type 2 update messages. To start a communication source, node will predict the geographical information of both the destination and the intermediate nodes. This step also is involved in predicting the delay as well. These predications are based on the result of update messages received from the destination and intermediate nodes. QoS routing is based on depth first search to find candidate routes satisfying the requirements. Geographically, shortest routes are being preferred. The disadvantage is that no resources are reserved on the path which in turn may lead to inaccurate delay prediction.

QAODV [23] specifies extensions which can be used to ensure maximum delay and minimum bandwidth along a route between a source and destination. Using the extensions in this document, AODV enables mobile nodes in an ad hoc network to specify, as part of a RREQ, Quality of Service requirements that a route to a destination must satisfy. In particular, a RREQ may include a QoS Object extension which includes bandwidth and delay parameters. In order to enable accumulated measurement for end-to-end delay, AODV also provides a Maximum Permissible Delay extension. If, after establishment of such a route, any node along the path detects that the requested Quality of Service parameters can no longer be maintained and that node must originate a ICMP QOS_LOST message back to the node which had originally requested the now unavailable parameters.

CEDAR [24] algorithm was basically designed for small and middle size network. CEDAR falls into reactive routing and core nodes are formed to perform the mechanism. These core nodes are selected by distributed algorithm and in a group of three hops where there is at least one core node. Transmission is done by these core nodes to their neighboring core node in the unicast manner. In the mobility of any core node, nodes attaching to it have to find another core node. CEDAR combines the support for QoS and routing. Subset of node is selected dynamically and distributed which maintains local topological information and route computation task. CEDAR protocol was defined to perform three-procedural task, that is, (1) self-organizing routing structure that is established and maintained for route computation, (2) unwavering higher bandwidth linking existing bandwidth information that is propagated to all core nodes whereas low bandwidth information of dynamic link is kept locally, and (3) QoS route computing using up-to-date local topology. The advantage of using CEDAR is that route discovery and maintenance tasks are limited to subset of nodes called core nodes which are easy to handle and low overhead is created. All the transmission lies on core nodes so it is the main disadvantage as well in case of core node movement or breakdown. This mobility affects the overall performance of the protocol.

SAODV [25] uses asymmetric cryptography to secure AODV routing messages. Route discovery mechanism is protected by using the security requirement features like data authentication, source authentication, importing authorization codes, and integrity. SAODV implies two mechanisms; that is, digital signatures are used to protect the nonmutable data in the RREQ and RREP messages and hash chains are used in SAODV to authenticate the hop count of the AODV routing messages (not only by the end points but by any node that receives one of those messages). A hash chain is formed by applying a one-way hash function repeatedly.

CSROR [26] uses different parameter from different layers employing the cross-layer information exchange mechanism. Destination node is responsible for selection of route on the basis of bandwidth, security, and energy. After the route request is initiated, these parameters are captured along the path for the resource aware and secure path establishment. Backup route is always maintained in case of any topological changes.

The rest of the paper is structured as follows. In Section 2, related works on different multipath routing protocol are summarized. In Section 3, proposed mechanism of adaptive cross-layer multimath routing protocol and its functionalities are given. Route discovery process details are explained in Section 4. Experimental results about simulation, parameters, and performance evaluation are presented in Section 5. Finally, conclusion and future work are given in Section 6.

2. Related Work

Some serious research has been carried out in MANET different aspects, ranging from routing, energy management, to security requirements, and so forth. MANET basic goal is to work in multihop fashion so that intermediate nodes forward packets to the destination. Therefore, intermediate nodes play an important role in MANET. Availability is the main focus in the overall performance of the network, which demands efficient routing mechanism for MANET. Large number of routing protocols have been developed, which can be broadly classified as table driven (proactive) and on-demand (reactive) schemes [27]. Another one combines the characteristics of both known as hybrid routing protocols. Proactive routing table searches for a path before anyone needs it. Reactive routing protocol searches for path whenever any node wants to send data to destination; however, both schemes have their own advantages and disadvantages. Our main focus of attention is reactive routing protocol. Reactive protocol works in two steps, that is, route discovery and route maintenance. In route discovery phase, whenever a source needs path to the destination, global flooding technique is used to detect all the possible paths to destination. Once all paths are discovered, source node selects one path to send the datagram packet to the destination. This single path selection is mostly done on the basis of shortest path. Shortest path generally follows the Bellman-Ford Algorithm, for example, OLSRBF [28]. The problem with the shortest path is that every node in the MANET will probably choose that path. This might become the center point of communication in most cases and more traffic passes through it. As a result more traffic yields more congestion and more delay [29]. This problem is solved by multipath routing.

Some or all paths can be utilized for sending data packet from source to the destination. Multipath protocols help in solving the congestion problem but add some complex questions as well. Once source gets all possible paths, there arises a need for mechanism for the selection of these paths; that is, how many paths are used? Some routing protocols make use of all paths available, while others tend to choose some of them based on certain criteria [30–33]. In efficient design of a protocol, there is always a tradeoff between the following parameters, that is, reliability, energy, delay, overhead, and so forth. Some of the energy efficient protocols are in [34–36].

Some of the cross-layer approaches used by the research community are listed. Reference [37] uses transport layer protocol version to simulate the effective increase in efficiency in terms of performance. Using the routing information at the transport level protocol, better throughput and end to end are achieved. Load of the nodes and mobility increase the lost packet, which will be minimized with the better interaction between transport protocol and routing information.

Several routing protocols have been proposed for multimedia traffic. Increase in use of multimedia applications forces the researcher to focus on the development of multimedia routing protocol. Several protocols have been tested that show good result for multimedia communication in MANET. Reference [38] considers that, with the aim of improving the performance of multimedia services over ad hoc systems, the use of cross-layer techniques could be the trend to follow.

MANET ability to work depends on the intermediate nodes cooperation and trust worthiness. In addition to nodes, some applications also need secure environment. A variety of secure routing protocols [39] have been developed to provide security in terms of detecting corruption from the nodes as well as reliability of the path. Protocols like [40] add the trust management [41] feature to the secure protocols. Reference [42] also presented a secure routing protocol based on cross-layer design and energy harvesting methods. Parameters are exchanges between different layers to get the knowledge of the states of node for efficient utilization of energy.

The proposed routing is adaptive in nature, that is, keeping in view the nature of the application; it selects two or more routes from source to destination. There is one default path, while other paths are based on available data rates, end-to-end delay, and security. Cross-layered mechanisms are used to exchange parameters across different layers. The protocol is taking care of the following three scenarios:

(i) Two or more than two default routes.

(ii) Two or more than two routes for multimedia applications.

(iii) Two or more than two secure routes for sensitive applications.

For better selection and optimization, cross-layer information is exchanged between different layers.

3. Proposed Mechanism

In MANET, there are many applications and may be a variety of scenarios. A single route selection mechanism may perform well in one scenario but may not in another. For example, AODV [9] routing protocol may perform well for simple applications but is not suitable for multimedia or such applications which need security. Similarly, CSROR [26] may work well to ensure some sort of security; however, it is not suitable for simple applications, which do not need security. Keeping in view wide range of applications and scenarios associated

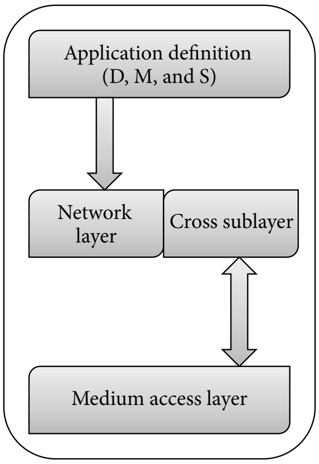


Figure 1: Proposed cross-layer architecture.

with MANETs, we propose an adaptive mechanism which decides multipath routes from source to destination by considering the type of application. The framework of the proposed scheme is given in Figure 1.

The proposed scheme defines the type of application at application layer, as D, M, and S, where

(i) D represents default application;

(ii) M represents multimedia application;

(iii) S represents secure application.

The proposed protocol always selects two or more than two optimum routes depending on type of application. The route selection process is adaptive and closely matches the application requirements. Different types of applications have different requirements. An optimum route is always selected by default; however, various applications can convey their individual requirements to the proposed protocol using few parameters such as bandwidth, delay, and security.

The default route is used for those applications which are nonsensitive and do not need more bandwidth. Default route selects the shortest path from source to destination similar to AODV.

Multimedia applications need such routes which have more bandwidth and minimum end-to-end delay. For such application, the proposed routing protocol selects two or more than two routes which are bandwidth rich having minimum delay from source to destination.

Secure route is selected when some sort of sensitive application is sent from source to destination. The proposed routing protocol takes care of network layer related security attacks.

In the proposed routing protocol, some important features are as follows:

(i) The type of application is defined by application layer.

(ii) Security module is working at network layer.

(iii) Bandwidth and end-to-end delay parameters are taken from medium access layer.

3.1. System Design

3.1.1. Basic Assumptions. We assume that, mostly, MANETs are established for three types of applications, that is, simple, multimedia, and applications having security concerned.

3.1.2. Basic Design. The proposed routing scheme uses two types of control packets for searching routes from source to destination:

(i) A broadcast route request packet.

(ii) A broadcast route reply packet.

The format of route request packet is given in Figure 2.

The route request packet consists of fields such as source ID, number of intermediate nodes, routing parameters, timer, and destination ID. The number of intermediate node fields increments itself with every intermediate node. Currently, we are using parameters up to $N3$, and the rest of subfields ($N4$, $N5$, and $N6$) are for future use. In case of a simple application which uses default routes, the parameters are assigned null values. The route request packet is discarded after expiry of the time value in timer field.

Route reply packet is similar to the route request packet.

3.1.3. Routing Table. The routing table consists of important information related to the path selection in accordance with the application. Typically, a routing table contains information such as destination address, hop count, and number of routes.

Routing table is shown in Table 2.

The routing table contains information of three paths from source to destination, so as to select at least two for sending data. As MANETs are mobile and dynamic networks, and routing paths are established and discarded regularly, the proposed scheme also discards routing table entries after expiry of timer.

3.1.4. Routing Parameters. The proposed scheme operates for three different types of scenarios having different parameters. Routing parameters are given in Table 3.

3.1.5. Cross-Layer Interface. A cross sublayer is defined which is used for exchanging cross-layer information as presented in Figure 1. Application layer defines the type of application, that is, default, secure, or multimedia, and the information is exchanged with the cross sublayer. Similarly, medium access layer provides information about available bandwidth and approximate delay. On the basis of the cross-layer information, the network layer selects multiple appropriate routes from source to destination.

4. Route Discovery Process

The adaptive route discovery process is discussed in this section.

Table 2: Routing table format.

Application type	Number of nodes	Parameter used	Source ID	Destination ID	Path 1	Path 2	Path 3	Timer

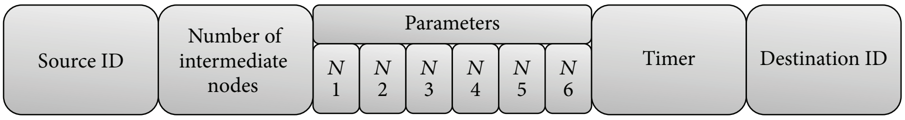


Figure 2: Packet format of route request.

Table 3: Application represented parameters.

Scenario/application	Parameter(s)
Default	Hop count
Security	Path reliability
Multimedia	Bandwidth and delay

4.1. Route Discovery Process (Default Route). Default route discovery process will be based on on-demand philosophy; that is, routes are discovered when needed. The route discovery process for default route is similar to AODV [9]. Two or more than two shortest routes from source to destination are selected among all available paths. Figure 3 demonstrates the flow of RREQ and RREP. Process will be started by source node initiation of the RREQ broadcast, also mentioning the number of paths desired by the application need. Intermediate nodes will broadcast the RREQ to their neighbors unless intermediate node is the destination node or knows a fresh path to the destination, in which case they are allowed to send the RREP. Destination node is allowed to reply according to the number of paths desired by the application. In case of N paths, destination node will reply to N RREQs. Destination will unicast the RREP to downstream neighbor which will further unicast till it reaches the source node. In case of any REER during transmission, new RREQ mechanism will be initiated by the source node. Flow chart of the mechanism is depicted in Figure 3.

4.2. Route Discovery Process (Multimedia Applications). Route discovery process for multimedia application will follow the procedure as mentioned in the default route but will take into account the parameter from different layer using the cross-layer mechanism, that is, bandwidth and delay. The destination node will here reply considering the maximum bandwidth and minimum delay. Flow chart is described in Figure 4.

4.3. Route Discovery Process (Secure). Route discovery process for secure application will follow the procedure as mentioned in the default route but will take into account the most secure path among all RREQ. Security algorithm will work on network layer. The destination node will reply to number of paths mentioned according to the preference mention in the security algorithm. Scenario of the flow of execution is given in Figure 5.

Combining algorithm of the mechanism is explained using pseudocode that is given in Algorithm 1. Route request module shows how the request will be generated after checking the sequence number. However, route reply will check the application and accordingly parameter will decide which path to choose.

4.4. Route Selection Process. Route selection process of the proposed scheme is discussed in detail in this section.

4.4.1. Default Route. Default routes will be searched if simple data needs to be transferred from source to destination; then two or more than two default routes are established between source and destination. These default routes will be the shortest routes among the available routes in terms of number of hops.

Path discovery for the default route is depicted in Figure 6. Source will send route request to its neighbor. Once all ROUTE-REQ are received by destination, the parameters are utilized in selecting the best path. In case of default route, shortest routes will be given preference. Destination will reply according to the set number of paths on shortest routes. Considering the shortest route according to number of hops, the destination node will reply to the two most suitable routes, that is,

Route 2 $\{n1, n7\}$,

Route 3 $\{n2, n7\}$.

4.4.2. Multimedia Application Route. Path discovery process for multimedia application is described in Figure 7, where route request is shown from source to destination. On receiving the route request, the destination will check the maximum bandwidth and less delay of all route requests.

Considering the high bandwidth and less delay, the three most suitable routes for multimedia application will be

(i) Route 7 $\{R3, R8, R14, R18\}$,

(ii) Route 8 $\{R3, R8, R13, R19\}$,

(iii) Route 9 $\{R3, R9, R12, R19\}$.

4.4.3. Secure Application Route. The proposed scheme uses multiple secure routes from source to destination. The mechanism prefers shortest paths. Our security approach is inspired from Confidant [43], which is capable of monitoring

```
Define App_Type, No_of _Paths;
Gen_RREQ()
{
If (no valid entry in route table for destination)
{RREQ is created with unknown Seq_No}
Else If (Have a valid destination in route table)
        {RREQ is created with last Seq_No}
SAVE [RREQ_ID]
Call Forward_RREQ()
}

Forward_RREQ()
{
If (Node listen a RREQ)
        {       If (Same as forwarded previously)
                                {    Discard;              }
                If (Node is destination) ‖ (Node has route to destination)
                                {    Send_RREP;
                                     Discard RREQ;        }
                Else            {    Forward_RREQ();          }
        }
}
Gen_RREP
{
        If (App_Type == "DEFAULT";)
        {
        Create number of reply according to No_of _Paths;
        Destination will unicast reply to the shortest paths;
        }
        If (App_Type == "MULTIMEDIA";)
        {
        Create number of reply according to No_of _Paths;
        Destination will unicast reply considering the maximum bandwidth and minimum delay;
        }
        If (App_Type == "SECURE";)
        {
        Create number of reply according to No_of _Paths;
        Destination will unicast reply considering the most secure path preference wise;
        }

}

Data_Transmission()
{
Source node will start transmission after receiving RREP
          If (RERR occur)
          {   Gen_RREQ();   }
}
```

Algorithm 1: Algorithm for generating route request and route reply.

and rating the nodes. When an anomalous node is detected, it is blacklisted and the proposed scheme avoids data forwarding through that particular node.

The architecture of the security module is given in Figure 8, where Reputation value (RV) is given to nodes describing the trust worthiness.

Secure route path discovery process is given in Figure 9. Route reply is based on the reputation value collected by route request along the path. Blacklisted nodes are ignored by destination node while generating route reply.

Considering the security mechanism adaptive by secure route protocol, the most suitable routes for secure application will be

$$\text{Route 1}\ \{N1, N5, N9, N12\},$$
$$\text{Route 2}\ \{N3, N7, N10, N13\}.$$

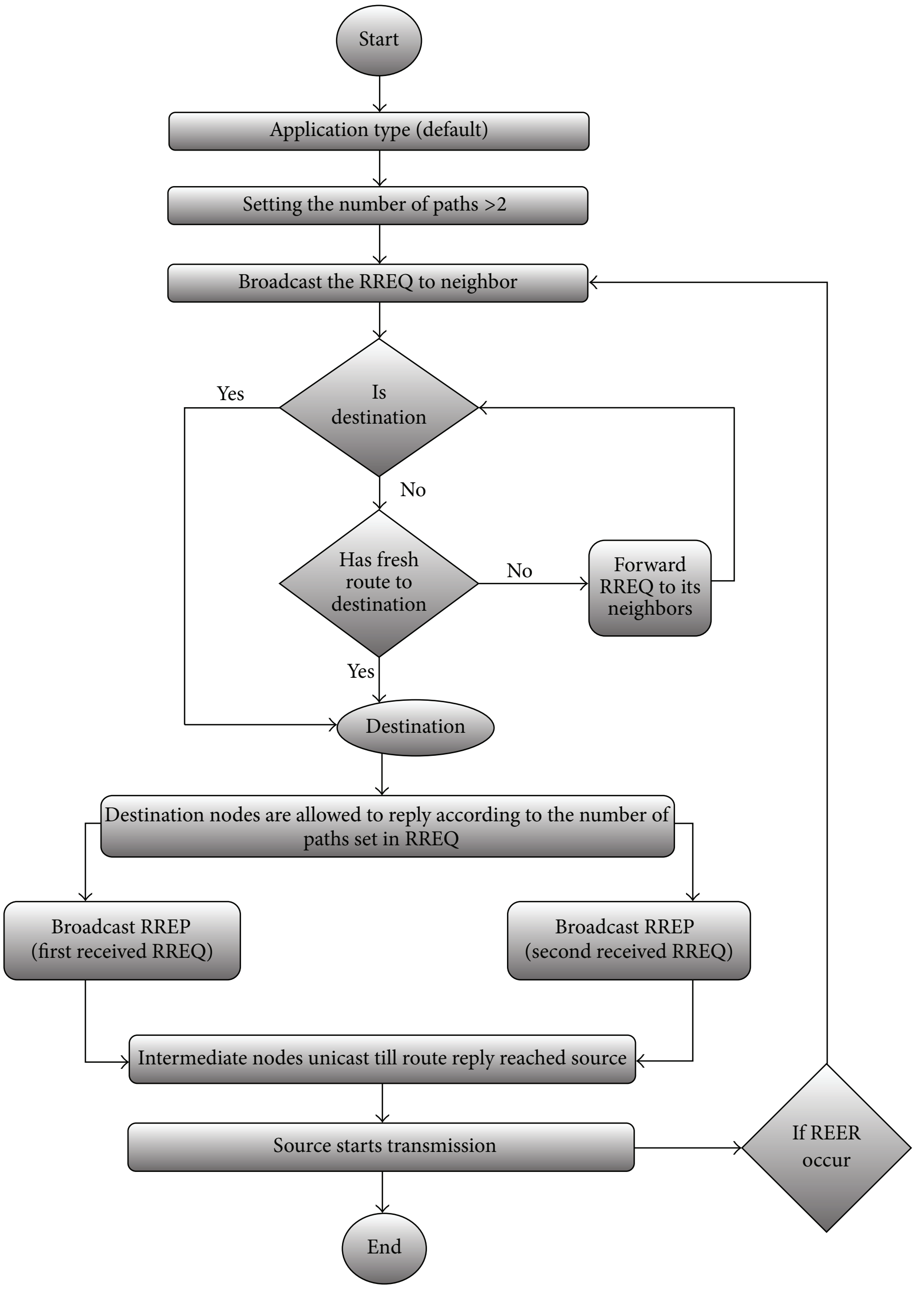

Start
Application type (default)
Setting the number of paths >2
Broadcast the RREQ to neighbor
Is destination
Yes
No
Has fresh route to destination
No
Forward RREQ to its neighbors
Yes
Destination
Destination nodes are allowed to reply according to the number of paths set in RREQ
Broadcast RREP (first received RREQ)
Broadcast RREP (second received RREQ)
Intermediate nodes unicast till route reply reached source
Source starts transmission
If REER occur
End

Figure 3: Flow of execution (default route).

5. Experimental Results

5.1. Simulation Parameters. In order to evaluate the performance of our proposed protocol, we conducted simulations in OPNET modeler 11.5. We used nodes based on 802.11 standards with different parameters given in Table 4.

Table 4: Simulation parameters.

Number of nodes	100, 200
Simulation time	3000 sec
Packet size	512 byte
Radio range	100 m
Maximum mobility	40 m/sec
Area	$1500 \cdot 500\ \text{m}^2$
Mobility model	Random waypoint

5.2. Simulation Result of Comparing with Each Other. First of all, we compared the different variants, that is, default, multimedia, and secure proposed routing protocol.

Media access delay is given in Figure 10. In this case, the default variant outperforms the other two, by having below 0.001 sec media access delay in the presence of 100 nodes. The secure variant has the highest end-to-end delay of 0.006 sec. The reason is that secure variant first needs to search a secure

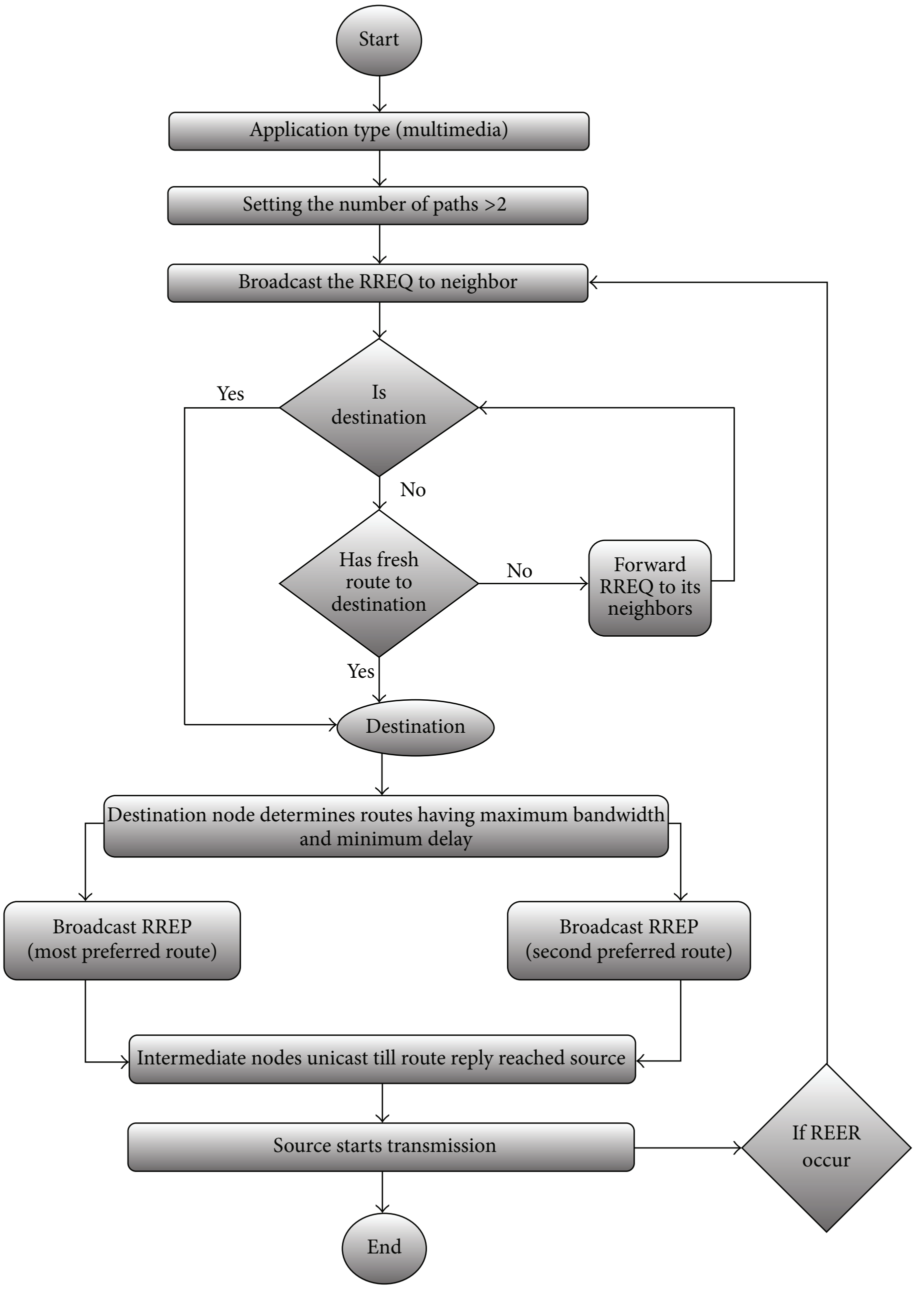

Start
Application type (multimedia)
Setting the number of paths >2
Broadcast the RREQ to neighbor
Is destination
Yes
No
Has fresh route to destination
No
Forward RREQ to its neighbors
Yes
Destination
Destination node determines routes having maximum bandwidth and minimum delay
Broadcast RREP (most preferred route)
Broadcast RREP (second preferred route)
Intermediate nodes unicast till route reply reached source
Source starts transmission
If REER occur
End

Figure 4: Flow of execution (multimedia applications route).

route from source to destination and then it will start packets transmission. On the other hand, multimedia variant has bandwidth parameters in its routing table, which enables it for immediate transmission from source to destination.

Route discovery efficiency of the three variants is given in Figure 11. In case of small numbers of intermediate nodes, all three variants have little difference in terms of searching routes from source to destination; however, as long as the number of nodes increases, the default variant becomes more stable as compared to the other two. The reason is that default variant searches the shorted paths from source to destination; therefore, it takes less time. On the other hand, secure and multimedia variants have to take care of different parameters to search routes.

In any network, more data drop occurs if more nodes are added. It is clear that the data drop is less when the numbers of intermediate nodes are less as shown in Figure 12. Multimedia variant is showing less data drop as compared to the other two. The reason is that multimedia variant takes care of the data rates/bandwidth. A routing path having more bandwidth will have less data drop as compared to the others. Default route has more data drop as it searches the shortest

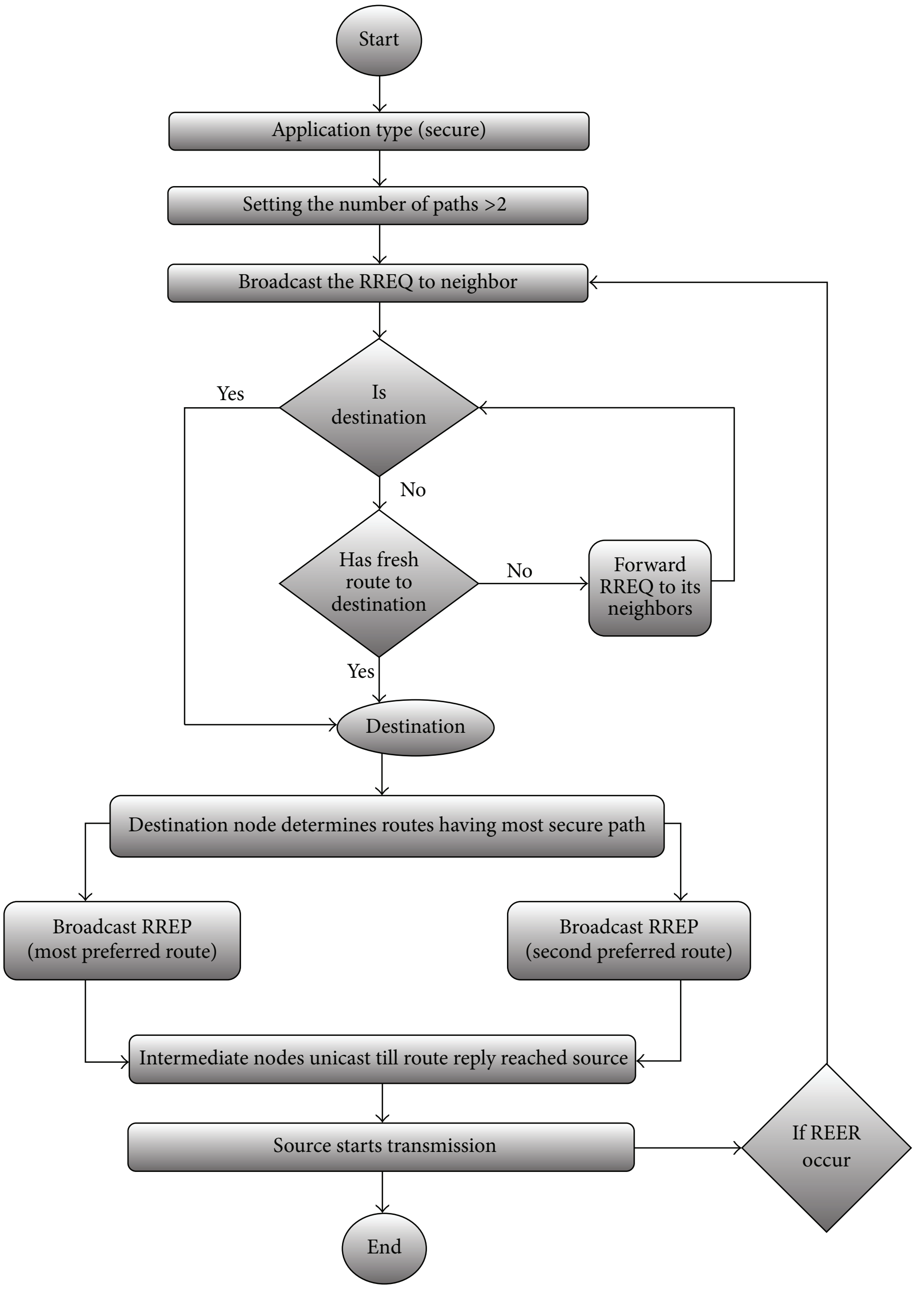

Start
Application type (secure)
Setting the number of paths >2
Broadcast the RREQ to neighbor
Is destination
Yes
No
Has fresh route to destination
No
Forward RREQ to its neighbors
Yes
Destination
Destination node determines routes having most secure path
Broadcast RREP (most preferred route)
Broadcast RREP (second preferred route)
Intermediate nodes unicast till route reply reached source
Source starts transmission
If REER occur
End

Figure 5: Flow of execution (secure route).

path from source to destination without considering available bandwidth and reliability of the selected routes. The shortest routes tend to be overloaded as well, hence dropping packets with higher ratio. Secure path shows average data drop as compared to the other two variants.

Routing overheads for a network of 100 nodes are given in Figure 13. These results show that the default variant has the smallest routing overheads as compared to the other two. The reason behind more routing overheads in multimedia and secure variants is that, both of them take care of additional parameters such as bandwidth and security for searching routes from source to destination. Such kind of searching generates more control packets as compared to default variant, which selects the shortest route without considering additional parameters.

Network load is mentioned as shown in Figure 14. These results show that default network load is low and stable as compared to the other two variants. Multimedia has the highest network load as the paths have to communicate bandwidth parameter constantly before transmitting while the secure route has intermediate load as compared to the other two.

In Figure 15, it is clear that as the number of packet grows the multimedia variant outperforms the other two.

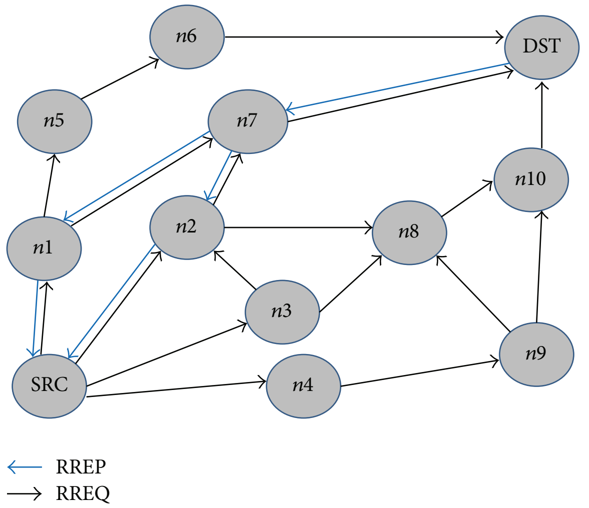


Figure 6: Path discovery process (default route).

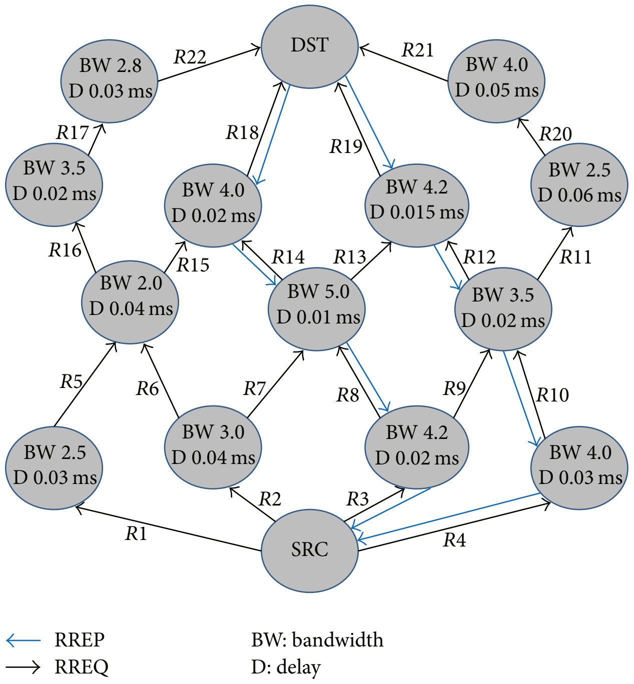


Figure 7: Path discovery process (multimedia application route).

The reason behind this is the bandwidth parameter taken by the multimedia application. The higher the bandwidth, the higher the number of packets transmitted. The default route just takes the shortest path into account which might not be useful for higher number of packets transmitted as the shortest paths are always congested, while the secure route is also considered the secure path not the fastest path.

5.3. Default Route Proposed Protocol Comparison with Different Protocol. Packet drop is shown in Figure 16 for 200 nodes. The comparison is made between DSR, AODV, OLSR, and proposed default routing protocol. It can be seen that DSR and OLSR have higher packer drop than AODV, whereas proposed default route outperforms AODV as well.

Figure 17 shows the network load in case of 200 nodes. AODV and proposed default route have approximately same network load. Initially, as more nodes are involved in routing, more control packets are shared among the network. With the increase in time, the network load is stabilized. Default protocol also outperforms other opponent protocols.

Medium access delay of DSR, AODV, OLSR, and proposed default route is shown in Figure 18 for 200 nodes. It depicts that single path medium access delay is less as compared to our proposed default protocol. Medium access delay of default protocol is higher as compared to others because it searches for multiple optimal paths instead of relying on a single path. This delay increased to some extent in the case when the number of nodes increases, as many nodes will be involved in path establishment.

Figure 19 illustrates the routing overhead for 200 nodes. It is found that routing overhead is lesser in proposed default protocol as compared to existing opponents like DSR, AODV, and OLSR. In case of proposed default protocol, a small number of control messages are exchanged, hence lesser routing overhead.

Figure 20 represents the route discover time for 200 nodes. It depicts that OLSR and DSR have smaller route discovery time as compared to AODV and proposed default protocol. With the increase in number of nodes the route discovery time reduces gradually for default protocol. Default protocol tends to perform well as the saturation of nodes increases.

5.4. Multimedia Route Proposed Protocol Comparison with Different Protocol. Similar set of experiments have been carried out for multimedia data considering the PLQBR, QAODV, and CEDAR as opponents. Figure 21 compares the packet drop for 200 nodes. Main reason of packet drop is due to mobility; whenever intermediate route is not able to find a route, the packet is dropped. Packet is dropped by source node if, after some attempts, it is unable to find the route or buffer overflow occurs. Less packet drops are experienced due to rich bandwidth available path.

Network load of large network is shown in Figure 22 for 200 nodes. PLQBR, QAODV, and CEDAR seem to have higher load, while proposed multimedia route has smaller impact on the network traffic. Proposed multimedia route selects path on the basis of higher bandwidth and lower delay which accomplished the network to stay healthy.

Medium access delay is depicted in Figure 23 for 200 nodes. Here, it is also clear that our proposed multimedia protocol delay is larger than the others due to multipath nature of protocol. The protocol takes some time to search for rich bandwidth aware and less delay path.

Routing overhead is the number of control packets that every node sends in order to get the knowledge of the network and establish paths. Routing overhead for 200 nodes is shown in Figure 24. These results show that CEDAR has higher overhead, whereas PLQBR and QAODV show better performance than CEDAR. However, proposed multimedia route

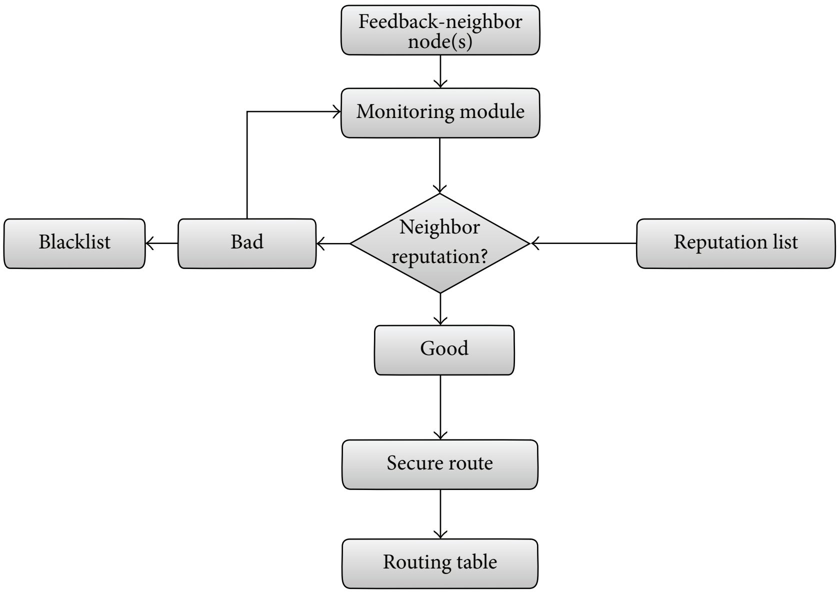


Figure 8: Architecture of the security module.

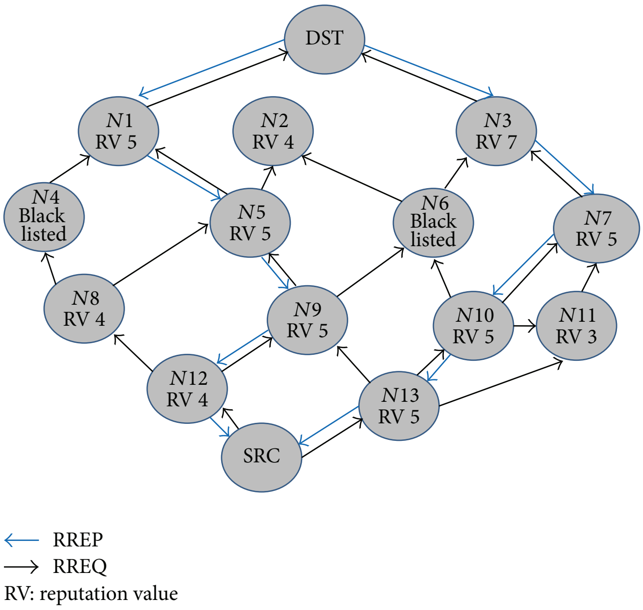


Figure 9: Path discovery process (secure route).

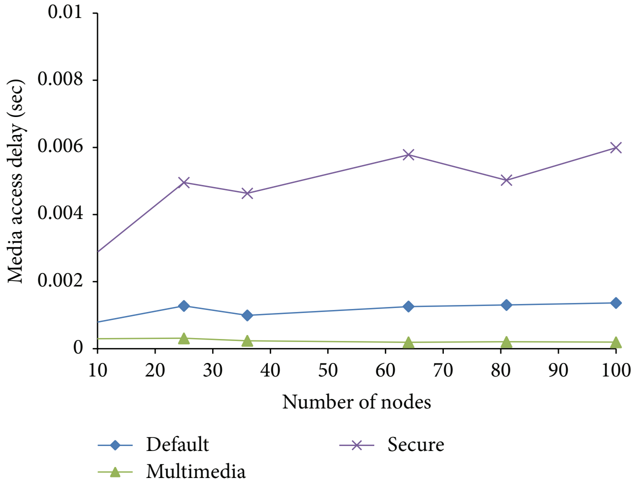


Figure 10: Media access delay for default, multimedia, and secure routes.

shows excellent result in both scenarios outperforming the other variant.

Route discovery time of PLBQR, QAODV, CEDAR, and multimedia protocol is described in Figure 25 for 200 nodes. It can be observed from Figure 25 that CEDAR is fast enough to beat its opponent; however, as the saturation of nodes increases, proposed multimedia variant is good enough to bring its discovery time to best level among all of them.

5.5. Different Protocol Comparison with Security Route Proposed Protocol. Figure 26 shows the packet delivery ratio at maximum speed between SAODV, CSROR, and proposed mechanism. SAODV delivery is decreased with the increase in speed. CSROR also shows the 77% delivery rate, whereas our proposed mechanism shows 88% delivery rate at all speeds.

Average delay at maximum speed is shown in Figure 27. Delay increases with the increase in mobility speed. SAODV has higher delay due to calculation of cryptographic algorithm, whereas CSROR performance is decreased with the increase in mobility. However, proposed secure routing protocol has 0.2 sec delay at maximum speed.

Routing overhead is mentioned in Figure 28 and shows that by increasing mobility the overhead will also be increased. However, proposed mechanism tends to show that

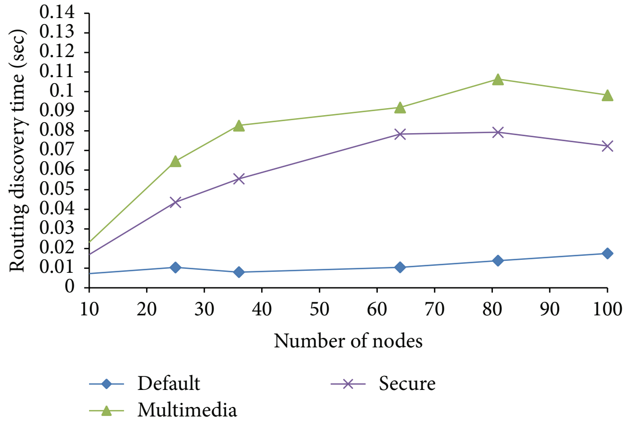


FIGURE 11: Route discovery time for default, multimedia, and secure routes.

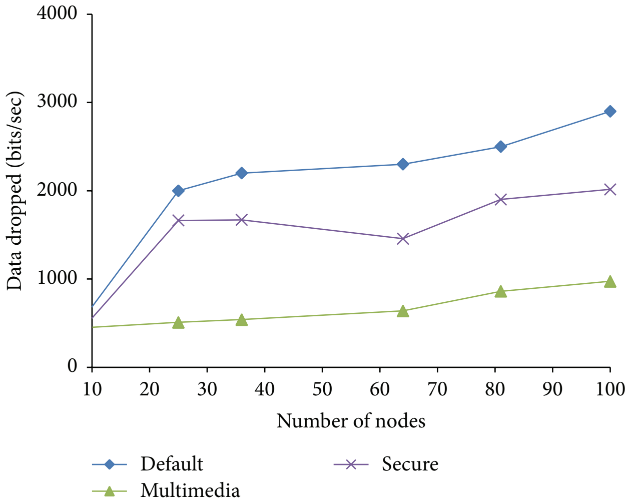


FIGURE 12: Data dropped in default, multimedia, and secure routes.

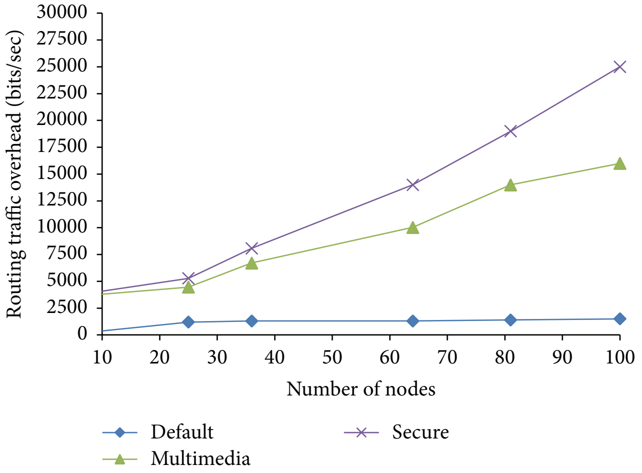


FIGURE 13: Routing traffic overhead time in default, multimedia, and secure routes.

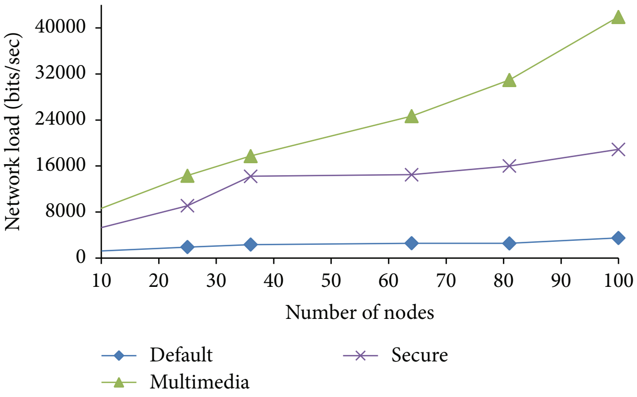


FIGURE 14: Network load in default, multimedia, and secure routes.

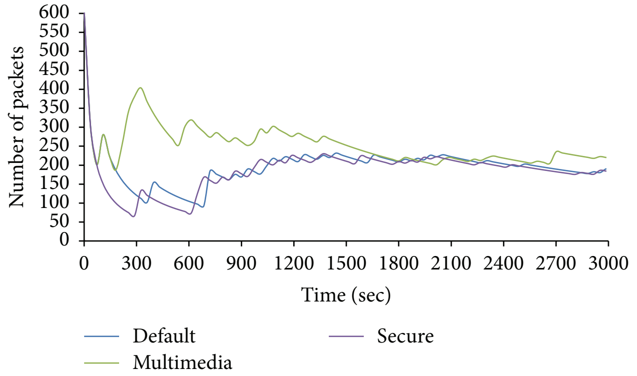


FIGURE 15: Number of packets sent in default, multimedia, and secure routes.

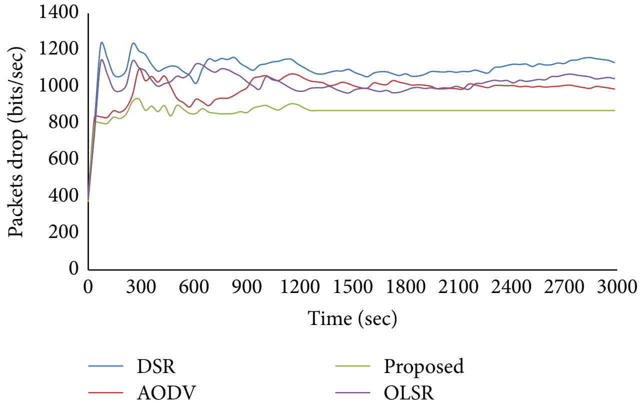


FIGURE 16: Packets drop (200 nodes).

overheard becomes stable after sometime showing no major variation.

The average end-to-end delay for a network in presence of malicious nodes is shown in Figure 29. Smallest end-to-end delay is observed in case of CSROR.SAODV that has slightly more end-to-end delay as compared to CSROR and proposed mechanism due to involvement of cryptographic operations in route discovery. In presence of malicious nodes, 0.5 sec delay is observed for proposed secure routing mechanism.

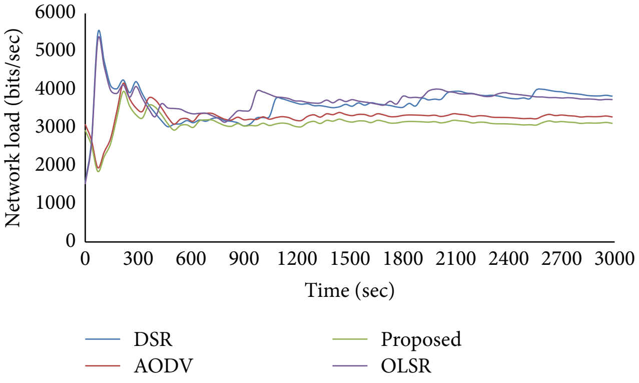


Figure 17: Network load performance (200 nodes).

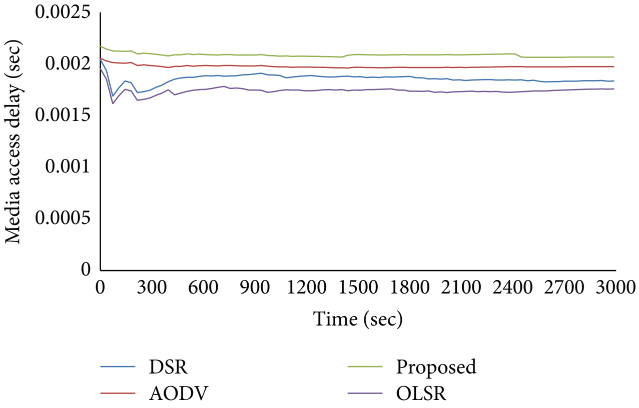


Figure 18: Media access delay (200 nodes).

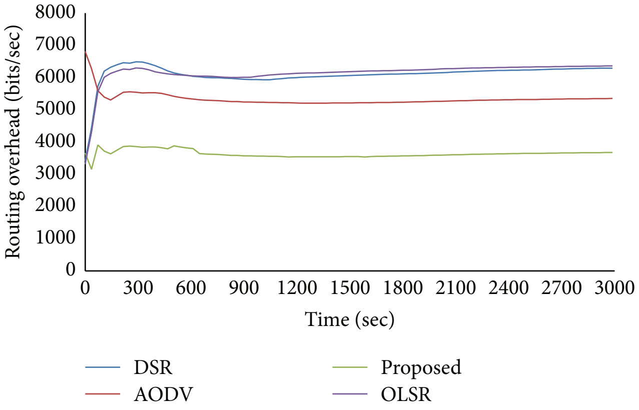


Figure 19: Routing overhead (200 nodes).

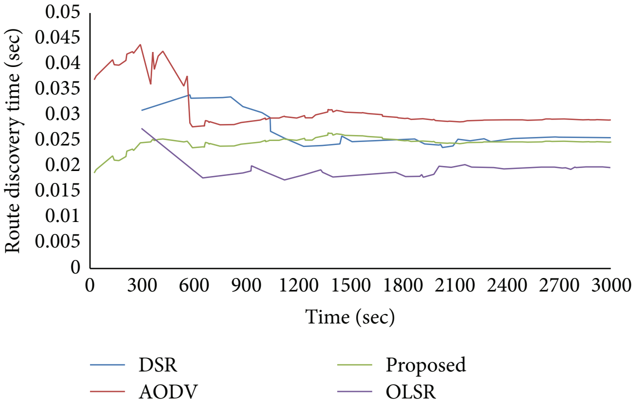


Figure 20: Route discovery time (200 nodes).

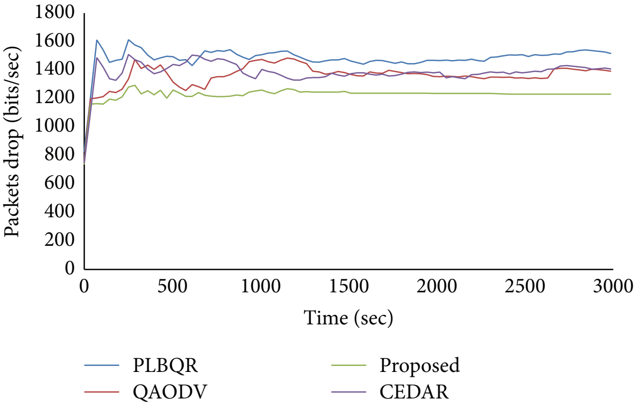


Figure 21: Packets drop (200 nodes).

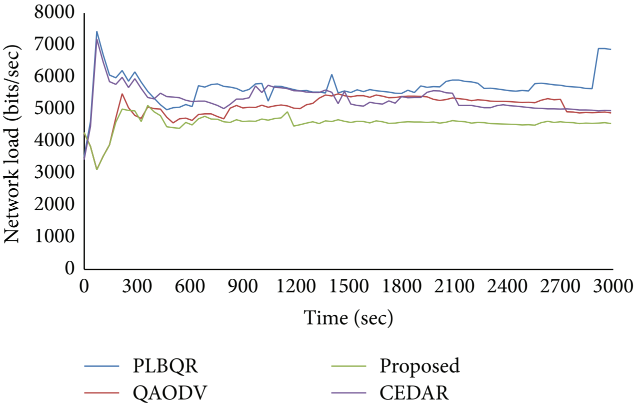


Figure 22: Network load performance (200 nodes).

In the presence of malicious nodes, average delay of proposed secure route, SAODV, and CSROR is mentioned in Figure 30, stating that CSROR performs well by providing less average delay than the other two opponents. Increasing pause time helps proposed mechanism in achieving less delay.

Packet delivery of secure proposed mechanism at maximum speed in presence of malicious nodes is also higher than CSROR and SAODV as shown in Figure 31. Packet delivery ratio is decreased to below 70% in SAODV and 80% in CSROR, while in the proposed mechanism it is approximately 85%.

The packet delivery ratio of CSROR, SAODV, and proposed protocol with pause time in the presence of malicious nodes is given in Figure 32. The packet delivery ratio of proposed protocol is approximately 85% more than CSROR and SAODV because of neglecting the malicious nodes.

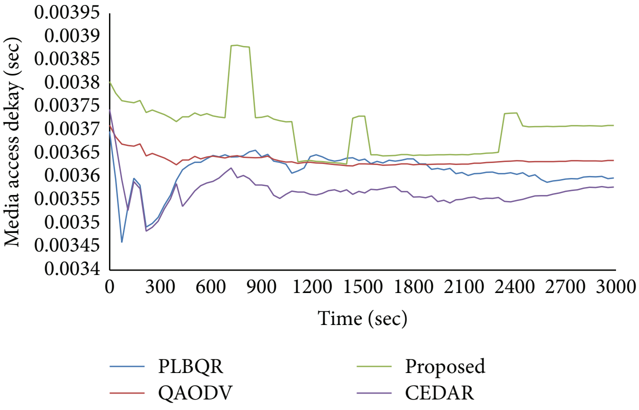


Figure 23: Media access delay (200 nodes).

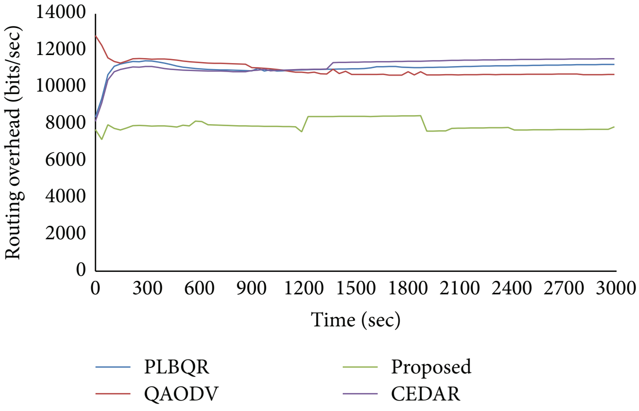


Figure 24: Routing overhead (200 nodes).

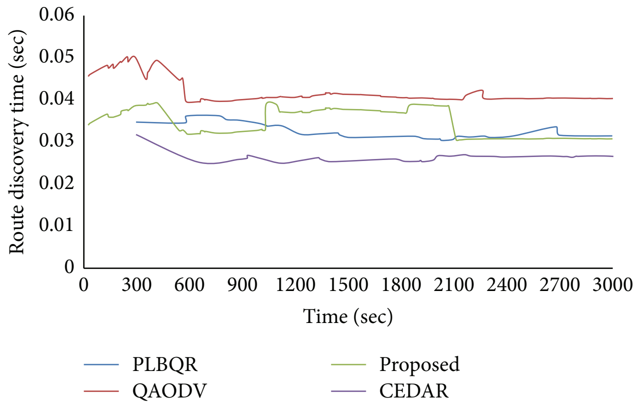


Figure 25: Route discovery time (200 nodes).

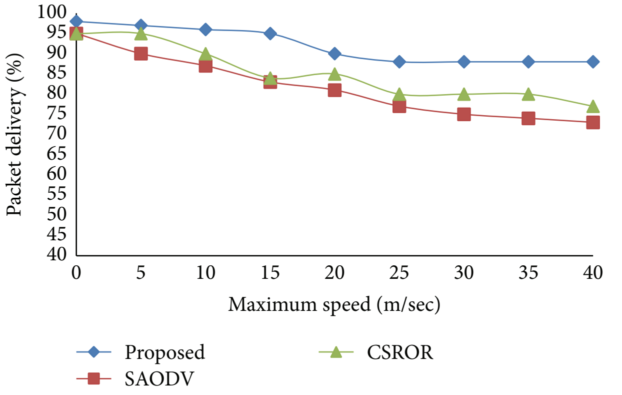


Figure 26: Packet delivery at maximum speed.

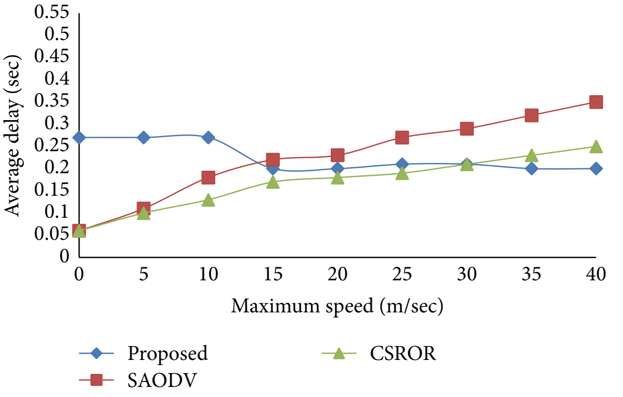


Figure 27: Average delay at maximum speed.

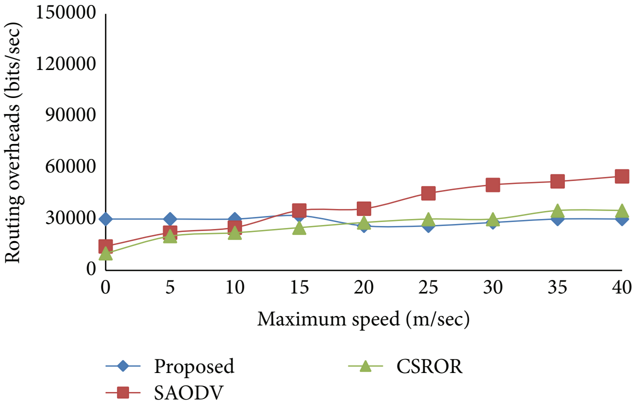


Figure 28: Routing overhead at maximum speed.

6. Conclusions and Future Work

In this paper, we presented cross-layer multipath routing protocol for MANET. The proposed protocol has two important features, that is, security and adaptive nature. These important features are achieved by multipath framework using cross-layer interface. Our proposed solution is capable of choosing multipaths by considering the type of application. The proposed protocol is compared with many existing protocols such as DSR, AODV, OLSR, CEDAR, PLQBR, QAODV, SAODV, and CSROR to evaluate three important application environments, that is, default applications, multimedia applications, and applications requiring security. The comparison covers most of the scenarios such as the packet delivery ratio, average delay, and routing overheads with

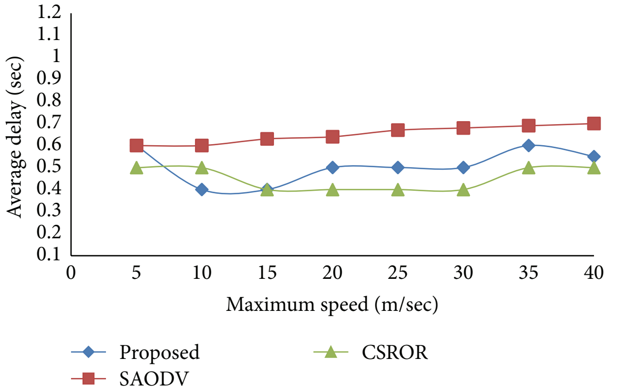


FIGURE 29: Average delay at maximum speed in presence of malicious nodes.

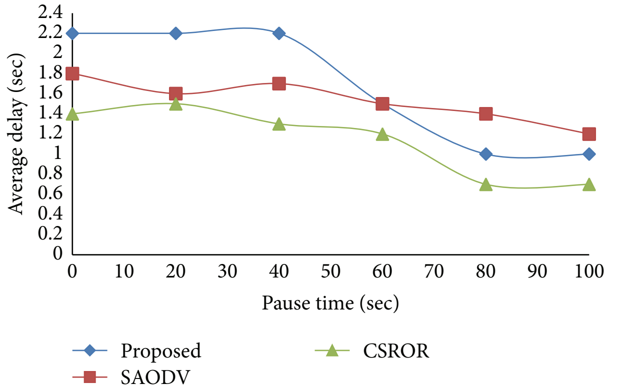


FIGURE 30: Average delay at pause time in presence of malicious nodes.

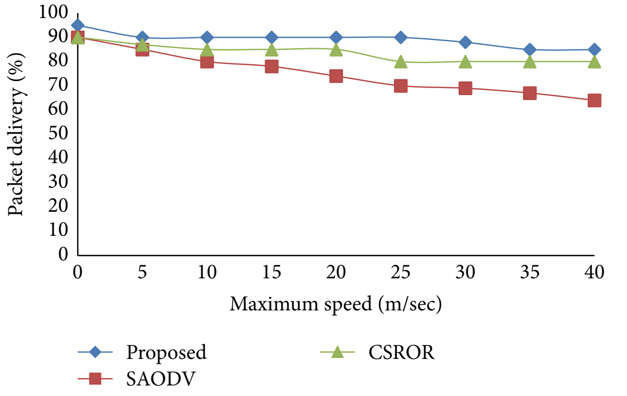


FIGURE 31: Packet delivery at maximum speed in presence of malicious nodes.

and without malicious nodes. The proposed protocol is very effective in most of the scenarios that we tested.

In future, we are planning to further strengthen the security of proposed routing scheme by introducing packet encryption and key exchange mechanism. Furthermore, we may consider to test and implement it in real scenarios.

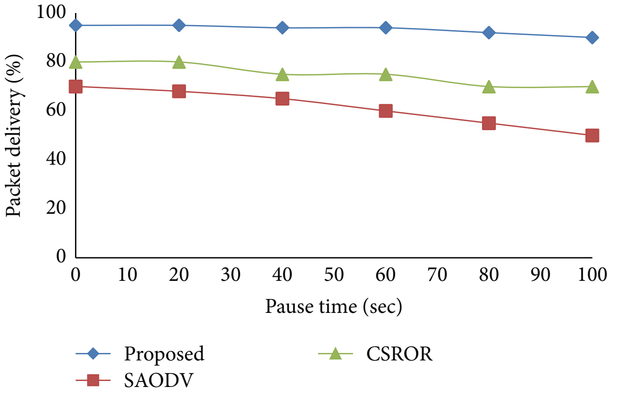


FIGURE 32: Packet delivery ratio with pause time in presence of malicious nodes.

Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

Acknowledgments

The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for funding this research group no. 037-1435-RG.

References

[1] L. Abusalah, A. Khokhar, and M. Guizani, “A survey of secure mobile Ad hoc routing protocols,” *IEEE Communications Surveys and Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.

[2] R. Lacuesta, M. Garcia, J. Lloret, and G. Palacios, “Study and performance of ad hoc routing protocols,” in *Mobile Ad Hoc Networks: Current Status and Future Trends*, pp. 71–101, CRC Press, Taylor and Francis, 2011.

[3] C. E. Perkins and P. Bhagwat, “Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers,” in *Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM ’94)*, pp. 234–244, London, UK, September 1994.

[4] S. Murthy and J. Garcia-Luna-Aceves, “An efficient routing protocol for wireless networks,” *Mobile Networks and Applications*, vol. 1, no. 2, pp. 183–197, 1996.

[5] G. Pei, M. Gerla, and T.-W. Chen, “Fisheye State Routing: a routing scheme for ad hoc wireless networks,” in *Proceedings of the IEEE International Conference on Communications (ICC ’00)*, pp. 70–74, New Orleans, La, USA, June 2000.

[6] J. J. Garcia-Luna-Aceves and M. Spohn, “Source-tree routing in wireless networks,” in *Proceedings of the 7th International Conference on Network Protocols (ICNP ’99)*, pp. 273–282, October-November 1999.

[7] G. Malkin and M. Steenstrup, “Distance-vector routing,” in *Routing in Communications Networks*, pp. 83–98, Prentice Hall, Englewood Cliffs, NJ, USA, 1995.

[8] J. Moy, “Link-state routing,” in *Link-State Routing, Routing in Communications Networks*, pp. 135–157, Prentice Hall, Englewood Cliffs, NY, USA, 1995.

[9] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pp. 90–100, New Orleans, La, USA, February 1999.

[10] D. Johnson, D. Maltz, and J. Broch, "DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks," in *Ad Hoc Networking*, pp. 139–172, Addison-Wesley, 2001.

[11] C.-K. Toh, "Associativity-Based routing for ad-hoc mobile networks," *Wireless Personal Communications*, vol. 4, no. 2, pp. 103–139, 1997.

[12] V. D. Park and M. S. Corson, "Highly adaptive distributed routing algorithm for mobile wireless networks," in *Proceedings of the 16th IEEE Annual Conference on Computer Communications (INFOCOM '97)*, pp. 1405–1413, April 1997.

[13] M. R. Pearlman and Z. J. Haas, "Determining the optimal configuration for the zone routing protocol," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1395–1414, 1999.

[14] T. Hamma, T. Katoh, B. B. Bista, and T. Takata, "An efficient ZHLS routing protocol for mobile ad HOC networks," in *Proceedings of the 17th International Conference on Database and Expert Systems Applications (DEXA '06)*, pp. 66–70, Krakow, Poland, September 2006.

[15] A. Kumar, D. Manjunath, and J. Kuri, *Communication Networking: an Analytical Approach*, Morgan Kaufmann, Los Altos, Calif, USA, 2004.

[16] S.-T. Chou, H.-T. Chern, C.-M. Shiao, and Z.-J. Lee, "Cross-layer design of AODV protocol for multi-hop flow in ad hoc network," *Ad-Hoc and Sensor Wireless Networks*, vol. 17, no. 3-4, pp. 233–252, 2013.

[17] M. M. Zoulikha and B. Amal, "Cross-layer approach among physical, MAC and routing layer in a shadowing environment," *Ad-Hoc and Sensor Wireless Networks*, vol. 21, no. 1-2, pp. 101–119, 2014.

[18] V. Carrascal, G. Delgado, and M. Igartua, "Multipath routing with layered coded video to provide QoS for video streaming applications over MANETs," in *Proceedings of the 14th IEEE International Conference on Communication Networks (ICON '06)*, pp. 1–6, Singapor, 2006.

[19] V. Loscrì, F. De Rango, and S. Marano, "Performance evaluation of on-demand multipath distance vector routing protocol over two MAC layers in mobile ad hoc networks," in *Proceedings of the 1st International Symposium on Wireless Communication Systems (ISWCS '04)*, pp. 413–417, September 2004.

[20] Y. Zhen, M.-Q. Wu, D.-P. Wu, Q.-J. Zhang, and C.-X. Xu, "Toward path reliability by using adaptive multi-path routing mechanism for multimedia service in mobile Ad-hoc network," *Journal of China Universities of Posts and Telecommunications*, vol. 17, no. 1, pp. 93–100, 2010.

[21] P. Jacquet and T. Clausen, *Optimized Link State Routing Protocol (OLSR)*, Internet Draft, IETF MANET Working Group, 2001.

[22] S. H. Shah and K. Nahrstedt, "Predictive location-based QoS routing in mobile ad hoc networks," in *Proceedings of the International Conference on Communications (ICC '02)*, vol. 2, pp. 1022–1027, May 2002.

[23] E. Royer and C. Perkins, "Quality of service for adhoc on-demand distance vector routing," IETF Internet Draft, July 2000.

[24] R. Sivakumar, P. Sinha, and V. Bharghavan, "CEDAR: a core-extraction distributed ad hoc routing algorithm," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1454–1465, 1999.

[25] M. G. Zapata, "Secure ad hoc on-demand distance vector routing," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 6, no. 3, p. 106, 2002.

[26] S. Khan and J. Loo, "Cross layer secure and resource-aware on-demand routing protocol for hybrid wireless mesh networks," *Wireless Personal Communications*, vol. 62, no. 1, pp. 201–214, 2012.

[27] V. Sharma and B. Alam, "Unicaste routing protocols in mobile ad hoc networks: a survey," *International Journal of Computer Applications*, vol. 51, no. 14, pp. 9–18, 2012.

[28] D. Tepsic, M. Veinovic, D. Zivkovic, and N. Ilic, "A novel proactive routing protocol in mobile ad hoc networks," *Ad-Hoc and Sensor Wireless Networks*, vol. 27, no. 3-4, pp. 239–261, 2015.

[29] M. Tarique, K. E. Tepe, S. Adibi, and S. Erfani, "Survey of multipath routing protocols for mobile ad hoc networks," *Journal of Network and Computer Applications*, vol. 32, no. 6, pp. 1125–1143, 2009.

[30] A. Tsirigos, Z. Haas, and S. Tabrizi, "Multipath routing in mobile ad hoc networks or how to route in the presence of frequent topology changes," in *Proceedings of the Military Communications Conference*, pp. 878–883, Vienna, Va, USA, October 2001.

[31] L. Wang, S. Jang, and T.-Y. Lee, "Redundant source routing for real-time services in ad hoc networks," in *Proceedings of the 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS '05)*, pp. 87–93, Washington, DC, USA, November 2005.

[32] S. Mao, S. Lin, Y. Wang, S. S. Panwar, and Y. Li, "Multipath video transport over ad hoc networks," *IEEE Wireless Communications*, vol. 12, no. 4, pp. 42–49, 2005.

[33] A. Nasipuri and S. Das, "On-demand multipath routing for mobile ad hoc networks," in *Proceedings of the 8th International Conference on Computer Communications and Networks*, pp. 64–70, IEEE, Boston, Mass, USA, 1999.

[34] Z.-t. Li, Q. Chen, G.-m. Zhu, Y.-j. Choi, and H. Sekiya, "A low latency, energy efficient mac protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 946587, 9 pages, 2015.

[35] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. S. Shen, "Energy and memory efficient clone detection in wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 5, pp. 1130–1143, 2016.

[36] M. Dong, K. Ota, A. Liu, and M. Guo, "Joint optimization of lifetime and transport delay under reliability constraint wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 27, no. 1, pp. 225–236, 2016.

[37] S. Hamrioui, P. Lorenz, J. Lloret, and M. Lalam, "A cross layer solution for better interactions between routing and transport protocols in MANET," *Journal of Computing and Information Technology*, vol. 21, no. 3, pp. 137–147, 2013.

[38] R. Sanchez-Iborra and M. Cano, "An approach to a cross layer-based QoE improvement for MANET routing protocols," *Network Protocols and Algorithms*, vol. 6, no. 3, pp. 18–34, 2014.

[39] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *IEEE Communications Surveys and Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.

[40] J. L. Tornos, J. L. Salazar, and J. J. Piles, "Secure trust management with source routing protocol for MANETs," *Network Protocols and Algorithms*, vol. 7, no. 2, pp. 42–59, 2015.

[41] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 13, no. 4, pp. 562–583, 2011.

[42] A. Nasipuri and S. Das, “On-demand multipath routing for mobile ad hoc networks,” in *Proceedings of the 8th International Conference on Computer Communications and Networks (IC3N ’99)*, pp. 64–70, Boston, Mass, USA, October 1999.

[43] S. Buchegger and J.-Y. Le Boudec, “Performance analysis of the CONFIDANT protocol (cooperation of nodes—fairness in dynamic ad-hoc networks),” in *Proceedings of the 3rd Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc ’02)*, pp. 226–236, ACM Press, Lausanne, Switzerland, June 2002.

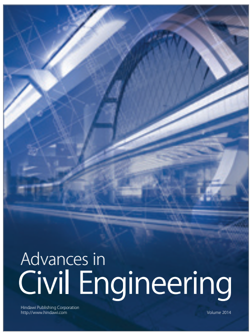
Journal of
Engineering

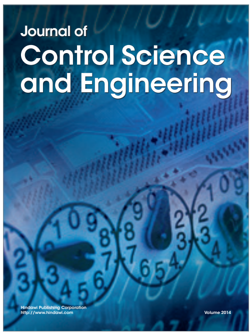
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

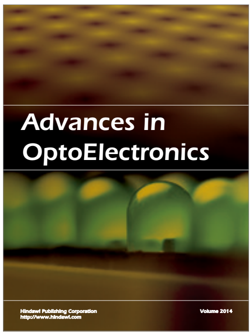
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

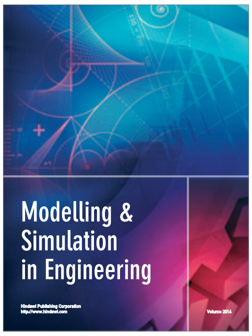
Journal of
Robotics

Journal of
Electrical and Computer Engineering

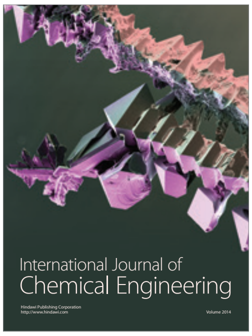

Advances in
OptoElectronics

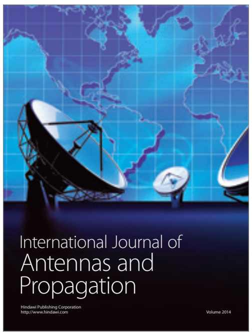
VLSI Design

International Journal of
Navigation and Observation

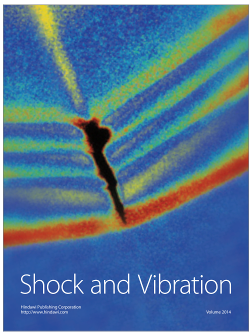

Modelling & Simulation in Engineering

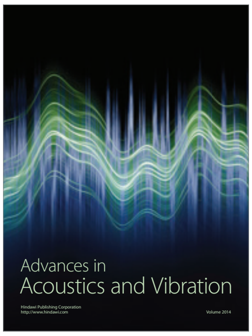
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration