1

Secure Multimedia Streaming over Multipath Wireless Ad hoc Network: Design and Implementation

Binod Vaidya[1], Joel J. P. C. Rodrigues[1,2] and Hyuk Lim[3]
[1]*Instituto de Telecomunicações, Covilhã, Portugal*
[2]*University of Beira Interior, Covilhã, Portugal*
[3]*Gwangju Institute of Science and Technology, Gwangju, Korea*

1. Introduction

Wireless ad hoc networks are becoming increasingly popular as they provide users access to information at anytime and from anywhere. A wireless ad hoc network is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies allowing people and devices to internetwork without any pre-existing communication infrastructure.

Furthermore, with an increase in the bandwidth of wireless channels and computational power of mobile devices, multimedia applications are expected to become more prevalent in wireless ad hoc networks in the near future. Examples of multimedia transmission over wireless ad hoc networks include multimedia streaming, transmitting audio and\or video in the battlefield as well as search and rescue operations after a disaster.

In mobile ad hoc network (MANET), several routing protocols such as Ad hoc On-demand Distance Vector (AODV) (Perkin *et al*., 2003) and Dynamic Source Routing (DSR) (Johnson *et al*., 2001) are widely used. However, the unreliability of the wireless medium and the dynamic topology due to nodes mobility or failure result to frequent communication failures, and high delays for path re-establishments, so single path routing may not be suitable for many applications, such as multimedia streaming and voice over Internet Protocol (VoIP).

In wireless ad hoc network, multipath routing is used to establish multiple paths between each source–destination pair. In fact, a multipath routing is a very promising alternative to single path routing as the former provides higher resilience to path breaks, alleviates network congestion through load balancing and reduces end-to-end delay (Mueller *et al*., 2004). Thus the multipath routing is highly appealing for multimedia streaming over wireless ad hoc networks.

Nonetheless, as security remains important factor that hinders the rapid deployment of multimedia applications over wireless ad hoc networks, security issue must be addressed in multipath multimedia streaming over wireless ad hoc networks.

In this chapter, we provide a generalized framework for secure and reliable multimedia streaming over multipath wireless ad hoc network. The aim of this chapter is to design and

implement a secure multipath routing scheme that can be efficiently utilized for multimedia streaming over wireless ad hoc network. This framework provides security not only for ad hoc routing but also for real-time data transfer. For securing multipath ad hoc routing and real-time data transfer, we have considered not only self-certified public keying technique and self-certificate but also digital signature and encryption technique. Moreover, we have considered Information Dispersal algorithm (IDA) in order to transmit real-time data through multiple paths.

The remainder of this chapter is organized as follows. Section 2 covers theoretical background mainly focused on issues in designing wireless ad hoc network and the existing works related to the proposed framework while Section 3 describes a framework for secure multipath multimedia streaming over wireless ad hoc network. Section 4 describes key distribution mechanism and Section 5 presents secure multiple route discovery scheme as well as real-time data forwarding scheme. Section 6 gives security analysis, whereas Section 7 exemplifies a performance evaluation of the proposed framework. Finally, Section 8 concludes the chapter.

2. Theoretical Background Theory

This section covers not only issues and challenges in designing wireless ad hoc network, but also some of the existing approaches for multipath routing in wireless ad hoc network, security framework for multipath wireless ad hoc network and multimedia transmission over wireless ad hoc network.

2.1 Issues in designing Wireless ad hoc network

While designing a wireless ad hoc network, we need to consider the following issues (Mohapatra & Krishnamurthy, 2004).

- Dynamic topology: The topology in a wireless ad hoc network may change randomly due to nodes' mobility. As nodes move in and out of the range of each other, some links break and new links are created.
- Multi-hop paths: Nodes inside an ad hoc network are often not within direct communication range. Thus the support of multi-hop paths is essential to the design of an ad hoc network. Also because of multi-hop paths, the end-to-end packet drop due to channel error is increased and the end-to-end throughput is greatly decreased, compared to the single-hop infrastructure based wireless networks.
- Unreliable wireless medium: The wireless communication medium has variable and unpredictable characteristics. Due to varying environmental conditions, such as different levels of electro-magnetic interference (EMI), the signal strength and propagation delay fluctuate with respect to time and environment.
- Self-organizing: The ad hoc network must autonomously determine its own configuration parameters including: addressing, routing, clustering, identification, power control, and etc.
- Energy conservation: Most ad hoc nodes, e.g. laptops, PDAs (Personal Digital Assistants) and sensors, have limited power supply, and cannot generate power themselves. Thus energy efficient protocols are critical for the longevity of the operation of the network.

- Scalability: Because of the extensive mobility and the lack of fixed infrastructure, pure ad hoc networks do not tolerate mobile IP or a fixed hierarchy structure. Thus, mobility, jointly with large scale is one of the most critical challenges in the design of ad hoc networks.
- Security: Because of the ability of the intruders to eavesdrop and jam/spoof the channel, the security problem of ad hoc networks is severe.

As a result of the above issues, a wireless ad hoc network is prone to numerous faults including:

- Transmission errors: Packets can be corrupted and dropped due to the unreliability of the wireless medium.
- Node failures: Nodes may fail at any time in the network. Nodes can also drop out of the network either voluntarily or when their energy is depleted.
- Link failures: Node failures and varying environmental conditions, e.g. increasing level of EMI, can cause links between two nodes broken. Both node and link failures can break a route, causing packet drop.
- Congestion: Depending on the topology of the network and the traffic flows, certain areas of the network can be congested, causing longer delays or packet loss.

Many different routing protocols have been proposed to solve the multi-hop routing problem in wireless ad hoc networks based on different assumptions and intuitions. Wireless ad hoc network routing must be simple and robust, and minimizes control message exchanges. On-demand routing protocols adapt well with dynamic topologies of the wireless ad hoc networks, due to their lower control overhead and quick response to route break. AODV (Perkin *et al*., 2003) and DSR (Johnson *et al*., 2001) are the most popular on-demand routing protocols in wireless ad hoc network. However, in a single-path routing, previously created multi-hop route could frequently break because of node mobility and interference. New route discovery would initiate for each failure, in turn, inducing routing overheads and latency. The topology of wireless ad hoc network is inherently volatile and routing algorithms must be robust against frequent topology changes caused by host movements.

A multipath routing protocol is a promising technique to overcome problems of frequent topological changes and link instability as the use of multiple paths could diminish effect of possible node and link failures.

2.2 Multipath routing in wireless ad hoc network

We briefly present the related works to multipath routing. DSR based multipath protocols (Leung *et al*., 2001; Lee & Gerla, 2001; Wang *et al*., 2001) as well as AODV based multipath protocols (Marina & Das, 2006; Ye et al., 2004; Lee & Gerla, 2000) have been proposed for wireless ad hoc networks.

Some of well-known multipath source routing protocols are Split Multipath Routing (SMR) (Lee & Gerla, 2001), and Multipath source routing (MSR) (Wang *et al*., 2001).

Split Multipath Routing (SMR) (Lee & Gerla, 2001) is one of the multipath extensions to DSR protocol. SMR is similar to DSR, and is used to construct maximally disjoint paths. It uses a modified route request (RREQ) packets flooding scheme in the process of route query. Duplicate RREQs are not necessarily discarded. Instead, intermediate nodes forward RREQs that are received through a different incoming link, and whose hop counts are not larger

than the previously received RREQs. By doing this, SMR increases the probability of two disjoint paths to the destination. Unlike DSR, intermediate nodes do not keep a route cache, and do not reply to RREQs. This is to allow the destination to receive all the routes so that it can select the maximally disjoint paths. Maximally disjoint paths have as few links or nodes in common as possible. The destination node returns the shortest path and another path that is maximally disjoint with the shortest path to the source node.
Multipath source routing (MSR) (Wang *et al*., 2001; Wang *et al*., 2002), is an extension of the on-demand DSR protocol. It consists of a scheme to distribute traffic among multiple routes in a network. MSR uses the same route discovery process as DSR with the exception that multiple paths can be returned, instead of only one. As in DSR, a source node will initiate a route discovery by flooding a RREQ packet throughout the network. Once the RREQ reaches the destination, a RREP will reverse the route in the route record of the RREQ and traverse back through this route. Each route is given a unique index and stored in the cache, so it is easy to pick multiple paths from there. Independence between paths is very important in multipath routing, therefore disjoint paths are preferred in MSR. Since source routing is used in MSR, intermediate nodes do nothing but forward the packet according to the route in the packet-header. The routes are all calculated at the source. A multiple-path table is used for the information of each different route to a destination. The traffic to a destination is distributed among multiple routes; the weight of a route simply represents the number of packets sent consecutively on that path.
However both these schemes do not include any security mechanisms.

2.3 Security mechanism in multipath wireless ad hoc network

Most of the routing protocols designed for wireless ad hoc networks generally assume all nodes in the network are cooperative and well behaving. But this assumption does not hold in many scenarios, in which routing information is vulnerable and misbehaving nodes could easily change the routing information to disrupt the network. Therefore, a number of secure routing protocols (Hu *et al.,* 2005; Sanzgiri *et al.,* 2005; Papadimitratos & Haas, 2002) have been proposed to prevent a set of attacks that attempt to compromise the route discovery. These protocols could be used to guarantee the acquisition of correct network topological information.
For securing multipath routing in the wireless ad hoc network, several protocols such as Secure Routing Protocol (SRP) (Papadimitratos & Haas, 2002), Secure Multipath Routing Protocol (SecMR) (Mavropodi *et al*., 2007) and Secure, Disjoint, Multipath Source Routing Protocol (SDMSR) (Berton *et al*., 2006) can be used.
Secure Routing Protocol (SRP) (Papadimitratos & Haas, 2002) assumes the shared symmetric key between the source and destination and data protection using Message Authentication Codes (MACs) in order to validate the authenticity and integrity. SRP is quite simple and lightweight solution, however, intermediary nodes are not authenticated, which leaves room for a lot of potential attacks. In fact one of the main security issues in SRP is that it has no defence against the invisible node attack (INA) (Marshall *et al*., 2003) that simply puts itself (and possibly a large number of other invisible nodes) somewhere along the message path without adding itself to the path, thereby causing potentially big problems as far as routing goes.
Mavropodi et al proposed an on-demand multipath routing protocol called Secure Multipath Routing (SecMR) (Mavropodi *et al*., 2007) protocol that can find multiple node

disjoint routes with protection against denial-of-service (DoS) attacks from a bounded number of collaborating insider attackers. However, the authors have mentioned that SecMR protocol does not fully protect from Man-In-Middle (MIM) and invisible node attacks.
Furthermore, these schemes do not consider secure real-time data transmission.
Earlier, Zhou and Haas (Zhou & Haas, 1999) proposed an approach using multiple routes between nodes to defend routing against denial-of-service (DoS) attacks. Then several protocols (Papadimitratos & Haas, 2006; Lou *et al*., 2009) using multiple paths between source and destination to provide secure data transmission in wireless ad hoc networks have been studied.
Secure Message Transmission Protocol (SMT) (Papadimitratos & Haas, 2006) proposed by Papadimitratos and Haas requires a security association between the source and the destination. SMT can operate with any underlying secure routing protocol. It uses Active Path Set (APS), a set of diverse, node disjoint paths to transfer dispersed pieces of each outgoing message using Information Dispersal Algorithm (IDA). The message and redundancy data are divided into a number of pieces so that if M out of N transmitted pieces are received successfully; the original message can be correctly reconstructed. The sender updates the rating of each path in its APS based on the feedback provided by the destination. The destination validates the incoming pieces and acknowledges the successfully received ones through a feedback across multiple routes back to the source. It can be seen that SMT provides limited protection against the use of compromised topological information, although its main focus is to safeguard the data forwarding operation. The use of multiple routes compensates for the use of partially incorrect routing information, rendering a compromised route equivalent to a route failure. Nevertheless, the disruption of the route discovery can still be the most effective way for adversaries to consistently compromise the communication of one or more pairs of nodes. Furthermore, SMT has not accounted re-sequencing mechanism.
Lou *et al*. presented a scheme called Security protocol for reliable data delivery (SPREAD) (Lou *et al*., 2009), which provides further protection to the existed data confidentiality service in an ad hoc network using multipath routing. It aims to protect secret message from being compromised. A secret message is transformed into multiple shares using the threshold secret sharing algorithm, are delivered via multiple node-disjoint paths to the destination. As the shares are delivered through multiple node-disjoint paths, the secret message as a whole is not compromised even if a small number of shares are compromised. However, as it mandates all the paths to deliver at least one share, the natural parallel redundancy of the multiple paths is reduced to serial redundancy and therefore, a malicious node dropping all packets or a broken link may disrupt the protocol. Moreover, SPREAD is not suitable for multimedia streaming, as it is not meant for real-time data transfer.

2.4 Multimedia transmission over multipath wireless ad hoc network

With an increase in the bandwidth of wireless channels and computational power of mobile devices, multimedia transmission over wireless ad hoc network is getting appealing. Nonetheless, the performance of real-time multimedia communication suffers from the quality variations of the wireless links in wireless ad hoc network. Thus the quality of real-time multimedia streaming is degenerated. The noisy communication channel can cause bit errors in the data transmission. This requires either additional redundancy or

retransmissions and therefore reduces the bandwidth. Moreover, fluctuations in the received signal strength due to interference or other changes in the environment can cause link failures. High delays or packet loss rates for the transmission are the consequence. The end user then gets bad quality in his received transmission, or even interruptions. This makes the deployment of real-time applications a challenging task. To overcome these challenges in multimedia transmission over wireless ad hoc network, several solutions (Mao *et al*., 2003; Wei & Zakhor, 2004; Hsieh *et al.,* 2007) have been proposed.

The authors in (Mao *et al*., 2003) introduced multi-stream coding with MultiPath Transport (MPT) for video traffic over ad hoc network. In their approach, a video bit stream is divided into several sub-streams by the video encoder and then packets from different substreams are sent over different paths.

The general architecture for multipath transport of video streams (Mao *et al*., 2003; Mao *et al*., 2005) is depicted in Fig. 1. At the sender, the raw video is compressed by a multi-stream encoder into *M* streams. Then the streams are partitioned and assigned to *K* paths by a traffic allocator. These paths are maintained by a multipath routing protocol. When the flows arrive at the receiver, they are first put into a re-sequencing buffer to restore the original order. Finally, the video data is extracted from the re-sequencing buffer to be decoded and displayed.

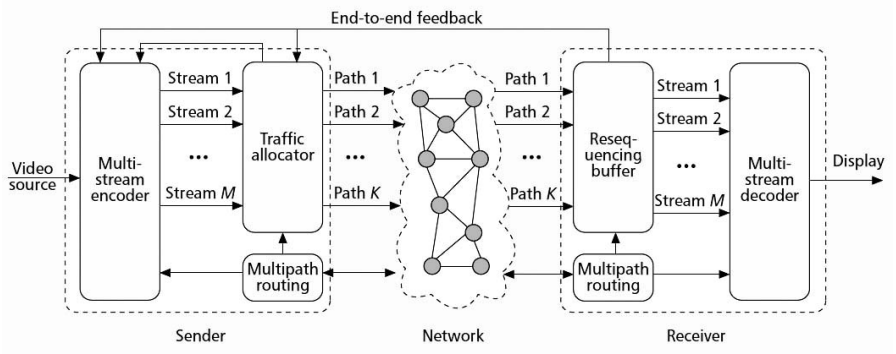

Fig. 1. General Architecture of multipath transport of video streams

Wei and Zakhor proposed Robust Multipath Source Routing Protocol (RMPSR) (Wei & Zakhor, 2004) that uses a per-packet allocation scheme to distribute video packets over two primary routes of two route sets, to support Multiple Description Coding (MDC) application over MANETs. And if one primary path is broken, it switches the transmission to another primary route.

Hsieh *et al.* (Hsieh *et al.,* 2007) presented an architecture supporting transmission of multiple of video streams in ad hoc networks by establishing multiple routing paths to provide additional video coding and transport schemes. In this framework, they have used on-demand multicast routing protocol to transport layered video streams.

However, these approaches do not consider any security measures.

3. Framework for Secure Multipath Multimedia Streaming over MANET

As the general architecture for the multipath transport of real-time multimedia applications depicted in the (Mao *et al.*, 2005) does not consider security measures, we have incorporated security enhancements in the framework for multipath multimedia streaming. The architecture for secure multipath multimedia streaming over wireless ad hoc network is shown in Fig. 2.

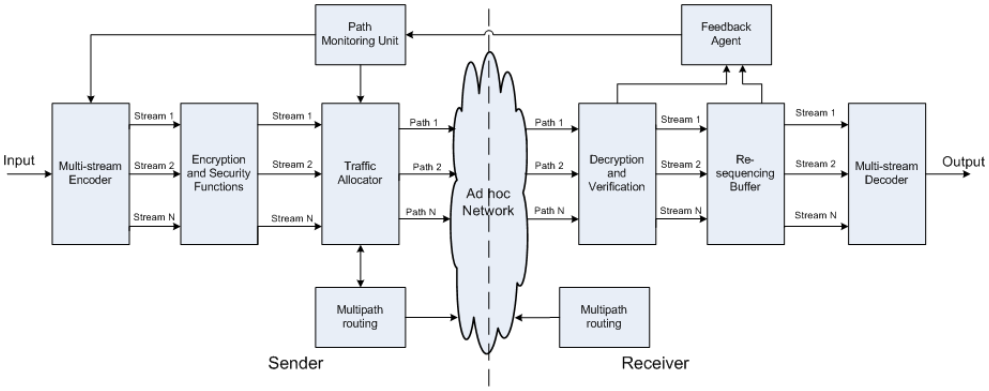

Fig. 2. Architecture of secure multipath multimedia streaming over wireless ad hoc network

We argue that proper selection of the active path set (APS) from the paths found by the multipath routing protocol can have a great impact on the usability of the found path-set in terms of both delivery ratio and delay and therefore will reduce not only the frequency of the costly route discovery process but also the overhead introduced to the network due to retry packets. Also, due to the dynamic topology of the network and existence of misbehaving nodes, which can change their behaviour through time, the paths will show time varying and non-stationary behaviour. Therefore, we maintain that any solution for improvement of the availability of end-to-end communication will not be successful unless it can adapt to the state of the paths and track their time varying behaviour.
For robust multiple routes discovery and data forwarding schemes in the presence of mobility and misbehaving nodes, the following assumptions have been considered:

- Source nodes and destination nodes are trustable, and between each pair of source node and destination node, there exists at least one route free of malicious nodes.
- Node-disjoint paths must be used to minimize the correlation between the paths.
- To control the overhead introduced to the network, an erasure coding or error-concealment source coding should be employed.
- It is assumed that the probability of the packets to be lost or modified is not the same for all paths.
- Due to variation of state of paths through time due to mobility or time varying misbehaviour of the malicious nodes; therefore, the system should be able to adapt to the current state of the paths.
- To guarantee the end-to-end confidentiality, end-to-end encryption must be used.

The function of each building block of the above-mentioned framework is presented as follows:

A. Multi-stream Coding Scheme
In the proposed framework, a multi-stream coding scheme is based on the Information Dispersal algorithm (IDA) (Rabin, 1989) to facilitate data redundancy. With this algorithm, the data and data redundancy is broken up into n streams, such that any m streams can be used to reconstruct data F, where n and m are positive integers, with m always less than or equal to n. If a sufficient number of streams are received at the destination, the destination proceeds to reconstruct the packets otherwise it waits.

B. Encryption & Security functions and Decryption & Verification
In the proposed framework, encryption & security functions at the sender side and decryption & verification at the receiver side are mainly for providing security for not only the route discovery but also for the real-time data transfer.

C. Traffic allocator
In this architecture, a traffic allocation scheme is used, which assigns the packets to the multiple paths using the weighted round-robin algorithm.
The list of active paths is maintained in the active path set (APS) table along with the path rating of each path. The path rating, r_s, is decreased by some constants each time failed transmission or unsuccessful transmission is reported, and it is increased by some constant for each successful reception. If the path rating falls below a threshold, the path is removed from the APS table.

D. Re-sequencing Buffer
One major concern when using multipath transport is the additional re-sequencing delay. Since packets sent on different paths suffer different delays, they may arrive at the receiver out-of-order. Thus the receiver needs to use a re-sequencing buffer to temporarily store the received fragments and put them in order using the sequence numbers.

E. Feedback agent
The main function of this agent is to collect the information of the received data and send a feedback message to the sender. The information of the received data can be either successful received, or unsuccessfully received due to modification or out-of-order, or never received because of packet loss due to congestion, wireless channel error, link breakage and/or misbehaving nodes.

F. Path Monitoring Unit
Monitoring scheme can adapt to the changes in the state of the paths. Depending upon the changes in the path, it would change the path cost which in turn change path rating. Here a path cost is the state of the path(s) describing the security and reliability related parameters of the path. For each path, we define two parameters reflecting availability and stability of the path. The parameters $a_i(t)$ and $s_i(t)$ denote the path availability and stability for all the paths respectively. These are stochastic representations of estimated reliability and stability of the i^{th} path among all available paths. Based on feedback message, the path cost is assigned with α^+, α^- and β^- for

successful delivery, packet loss, and modification respectively. It shows the path behavior in last packet transmission.

G. Multipath routing
The problem addressed by multipath routing protocols in the above-mentioned architecture is how to build multiple paths, in order to maximize the received video quality at the receive side. The key issue for the success of multipath streaming is to make packet loss over multiple paths as uncorrelated as possible. One natural metric for selecting multiple paths is to require them to be node-disjoint. Packet loss due to link failure or path breakage caused by nodes' movement are independent among node disjoint paths.

4. Key Distribution Mechanism

In this section, we describe key distribution mechanism used in the proposed framework that is based on self-certified key cryptography (Girault, 1991). In this regard, the self-certificate (Lee & Kim, 2000) for self-certified key is considered, which can provide the authenticity of self-certified key. Table 1 shows the notations used in key distribution mechanism.

Notation	Description
x_X	private key of node X
y_X	public key of node X
k_X	random number choosen by node X
CI_X	Certificate Information for node X
r_X	commitment of node X
ID_X	Identity of node X
CN	Certificate number
t_e	Certificate expiry time
s_X	signature parameter for node X
$h()$	hash function
$sCert_X$	Self-certificate generated by node X
$Sig_{x_X}(M)$	Message M digitally signed by node X

Table 1. Notations used in the key distribution mechanism

Initially, a centralized authority (CA) chooses random number x_{CA}, which is its private key and the corresponding public key is computed as $y_{CA} = g^{x_{CA}}$. It is assumed that y_{CA} is known to all the nodes presented in the network.
Prior to joining the network, the mobile node (MN) must connect to the trusted Certificate Authority (CA). This process is done offline. Suppose a node A joins the network, it will obtain the self-certified key from CA and then generate self-certificate, which is as follows.

1. CA chooses $\tilde{k}_A$.
2. CA computes $\tilde{r} = g^{\tilde{k}_A}$ and sends it to a node A.

3. The node A chooses a and computes $r_A = \tilde{r}_A g^a$
4. The node A sends ID_A, r_A to CA.
5. CA creates $CI_A = [ID_A \| r_A \| ID_{CA} \| y_{CA} \| CN \| t_e]$
6. CA computes $\tilde{s}_A = x_{CA} h(CI_A) + \tilde{k}_A$ and it to the node A.
7. The node A obtains its private key $x_A = \tilde{s}_A + a$
8. The node A verifies CA's signature by $y_A = g^{x_A} = y_{CA}^{h(CI_A)} r_A$
9. The node A then generates $sCert_A = Sig_{x_A}(CI_A, y_A)$

When node A presents $sCert_A$, any node in the network can explicitly verify the validity of y_A as follows.

1. Check the validity of node A's signature in $sCert_A = Sig_{x_A}(CI_A, y_A)$ by y_A.
2. Check the validity of CA's certification by checking $y_A = g^{x_A} = y_{CA}^{h(CI_A)} r_A$

5. Secure Multipath Routing Scheme

In this section, we propose a secure framework for multipath wireless mobile ad hoc networks that provides end-to-end security between the source-destination pair. The main goal of this framework is to provide security not only on the multipath routing protocol between the source and destination nodes but also on data transmission using these multiple routes.

This proposed framework is designed on based of source routing as such DSR. The proposed framework has three basic operations: route discovery, real-time data transmitting and route maintenance.

For provisioning security in route discovery phase, we have considered self-certified public key that can be used to generate self-certificate and digital signature, whereas used session keys to encrypt real-time data during real-time data transfer phase.

Before we discuss about the proposed framework further, we provide some of the assumption we have made for this scheme:

- We assume that a source node (S) and a destination node (D) share some secret information between them. For example, a source node knows a destination node's public key. For the key distribution, we have considered self-certified public keying technique (Girault, 1991; Lee & Kim, 2000), so any node in the network can compute another node's public key knowing public parameter, ID and CA's public key.
- We assume bidirectional communication on each link. This assumption is justified, since many wireless media access control (MAC-layer) protocols, including IEEE 802.11, require bidirectional communication.
- We assume that a mobile node can communicate with only neighbouring nodes and maintains the list of all its current immediate neighbouring nodes. However, secure neighbour discovery would only serve to strengthen the security of this scheme.

Table 2 shows the notations used in the proposed secure multipath route discovery for wireless ad hoc network.

Notation	Description
Sq	Unique ID assigned by S to RREQ
$Sign_{K_X-}(M)$	Message M digitally signed by node X
$sCert_X$	Self-certificate generated by node X
N_S	Nonce by S
SK_S, SK_D	Session keys generated by S & D

Table 2. Notations used in the multipath route discovery

5.1 Route Discovery

Route Discovery for multipath routing in wireless multihop ad hoc network is as follows: The route from source S to destination D will be obtained by flooding the network with route request (RREQ) packets.

When a node receives an RREQ packet with source address S and destination address D, it looks at its Intermediate node table. Intermediate node table maintains the list of recent most RREQ received for any source destination pair and the intermediate nodes for the request. If the packet arrived has a list of intermediate nodes that is a superset of what is there in the routing table, the packet is discarded else the node adds its own entry into the packet and rebroadcasts it.

Suppose an intermediate node 1 receives the RREQ directly from *S*. When the same RREQ packet with intermediate nodes {2} arrive from 2, *1* discards it. Upon receiving the RREQ, node *1* appends its address in route list and self-certificate, then rebroadcasts it.

In case of node *4*, it will accept RREQ from neighbors and 2, however discard that from node 5. Upon receiving the RREQ from node *1*, node *4* verfies the $sCert_1$, If it is valid, node *4* removes the signature of node *1* and signs the RREQ message with its K_{4-} and replaces $sCert_1$ with its $sCert_4$. And it appends its address in route list then rebroadcasts it.

Route request process is as follows:

$$S \Rightarrow *: \quad \left\langle Sign_{K_{S-}}(REQ,S,D,Sq),\ route\_list, E_{K_{D+}}(N_S,SK_S), sCert_S \right\rangle$$

$$1 \Rightarrow *: \quad \left\langle Sign_{K_{1-}}\left(Sign_{K_{S-}}(REQ,S,D,Sq),\ route\_list, E_{K_{D+}}(N_S,SK_S), sCert_S\right) sCert_1 \right\rangle$$

$$4 \Rightarrow *: \quad \left\langle Sign_{K_{4-}}\left(Sign_{K_{S-}}(REQ,S,D,Sq),\ route\_list, E_{K_{D+}}(N_S,SK_S), sCert_S\right) sCert_4 \right\rangle$$

$$7 \Rightarrow *: \quad \left\langle Sign_{K_{7-}}\left(Sign_{K_{S-}}(REQ,S,D,Sq),\ route\_list, E_{K_{D+}}(N_S,SK_S), sCert_S\right) sCert_7 \right\rangle$$

Route request process in Route Discovery is shown in Fig. 3.

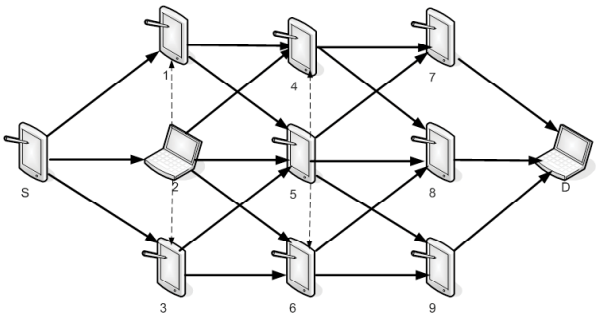

Fig. 3. Route Request Processing

When D receives RREQ packets from its neighbouring nodes, it is responsible for discovering multiple paths - primary path and node disjoint paths from all the received routes.
When receiving the first RREQ, the destination verifies all the signatures and caches the route list. It decrypts and stores session key from S.
Then D generates route reply (RREP) packet, which includes accumulated route as obtained from RREQ, a digital signature of the D on the entire message, and encrypted session key SK_D. The RREP is then sent back on the reverse route as given by the accumulated route in the RREQ. Each intermediate node on the reverse route verifies that its identifier as well as the predecessor and successor nodes' identifiers in the accumulated route.
If both tests are valid, the intermediate node signs the RREP and passes it to the next node in the path. As a result, the RREP reaches the source node. This node verifies whether it received the message from its neighbour and if this neighbour is the first node on the path. The path is then accepted to be valid if all the signatures are verified. It also decrypts and stores the session key from destination.
Route reply process is as follows:

$D \Rightarrow 7: \quad \langle Sign_{K_{D^-}}(REP, S, D, Sq, N_S, route\ list), E_{K_{S^+}}(S_{K_D}), sCert_D \rangle$

$7 \Rightarrow 4: \quad \langle Sign_{K_{7^-}}(Sign_{K_{D^-}}(REP, S, D, Sq, N_S, route\ list), E_{K_{S^+}}(S_{K_D}), sCert_D), sCert_7 \rangle$

$4 \Rightarrow 1: \quad \langle Sign_{K_{4^-}}(Sign_{K_{D^-}}(REP, S, D, Sq, N_S, route\ list), E_{K_{S^+}}(S_{K_D}), sCert_D), sCert_4 \rangle$

$1 \Rightarrow S: \quad \langle Sign_{K_{1^-}}(Sign_{K_{D^-}}(REP, S, D, Sq, N_S, route\ list), E_{K_{S^+}}(S_{K_D}), sCert_D), sCert_1 \rangle$

When the destination receives a duplicate RREQ, it will compare route path of RREQ to its route cache. If only source and destination nodes are same, a path is a node-disjoint path; otherwise it will discard the RREQ.

5.2 Route Maintenance

Whenever a route breaks because of node mobility, the neighbor of the node will send a route error to the source. The source will then discard that route from the routing table. If the source has another path to the destination, it can use it. When the source has no entry for the destination and the session is still active, it would initiate a new route discovery.
In order to authenticate the packet and ensure freshness, this scheme uses digital signature along with a nonce in route error messages.

5.3 Real-time Data Transmitting

Protecting the routing message from attacks is only one part of the security mechanisms of an ad hoc network. Often, a malicious node may behave normally during route discovery phase, however, during data forwarding phase, it either drops the segment packet or modifies the content of the packet and then forwards it.

The proposed scheme provides secure multipath data forwarding. In data forwarding, session keys SK_S and SK_D are used to encrypt and hash packets transmitted respectively. Apart from doing encryption and hashing, the packets would be divided in n fragments that would be sent to the destination on n different routes. The notations used in secure real-time data transfer are shown in Table 3.

Notation	Description
N	Sequence number
$h()$	hash function
TS	Timestamp
$E_{K_{X+}}(M)$	Encryption of message M with K_{X+}
$D_{K_{X-}}(M)$	Decryption of message M with K_{X-}
SK_S, SK_D	Session keys generated by S & D

Table 3. Notations used in secure real-time data transfer

To send multimedia data M from the source S to destination D,

1. S divides the packet in a set of n streams $\{g_0, g_1, ..., g_{n-1}\}$ with redundancy factor r. Thus the resultant length of each stream would be
$$len(g_i) = r \times \frac{len(M)}{n}; \quad 0 \le i < n$$
2. It encrypts each stream with SK_S i.e. it calculates encrypted stream as
$$E_{g_i} = E_{SK_S}(g_i \,||\, i \,||\, n \,||\, N \,||\, TS); \quad 0 \le i < n$$
3. It computes $h\left(E_{g_i} \,||\, SK_D\right)$
4. It sends $E_{g_i} \,||\, h\left(E_{g_i} \,||\, SK_D\right)$ to D on path i.
5. If S receives an acknowledgement from D with some successful delivered, some unsuccessfully delivered and some lost fragments, it resends the unsuccessful fragment and lost fragment on another path.

When D receives any packet from S from path i.

1. D generates $h\left(E_{g_i} \,||\, SK_D\right)$
2. It compares generated hash with the received one. If they match, the packet must be from S and not from any other node. If not, it informs the feedback agent.
3. It decrypts packet i.e. it calculates $g_i \,||\, i \,||\, n \,||\, N \,||\, TS = D_{SK_S}\left(E_{g_i}\right)$.
4. It checks timestamp.

5. As soon as D receives sufficient packets with sequence number *N* and different *i*'s, it reconstructs *M*.
6. If D doesn't receive enough packets to reconstruct *M* till the receiver timer expires, it sends the acknowledgement of the received fragments to S.

6. Security Analysis

A lot of attacks are possible in wireless mobile ad hoc networks that could threaten the security of the network (Pervaiz et al., 2007). We will evaluate the proposed scheme for passive attacks and active attacks.

A. Active attacks:

In active attacks, an attacker actively participates in disrupting the normal operation of the network services. A malicious host can create an active attack by modifying packets or by introducing false information in the ad hoc network. It confuses routing procedures and degrades network performance. Thus the attacks can carry the different detriments that focus on impersonation, modification, fabrication, replay, denial of service, and disclosure attacks (Mishra, 2008).

In this scheme, every intermediate node uses digital signature for authentication; source and destination nodes also use their certificates and session keys to authenticate and communicate securely. Therefore, this scheme is resilient to several active attacks such as attacks due to impersonation, modification and fabrication. For instance, a malicious node may cause fabrication attacks by falsifying route error (RERR) messages. This scheme defeats the RERR fabrication attack as it uses digital signature for protecting RERR messages and ensures authenticity and integrity of RERR messages. Similarly, a malicious node may try to impersonate a source node, however, this attempt will not be successful as the source node uses its digital signature to secure the non-mutable parts in RREQ message. Furthermore, since the scheme uses explicit self-certified public keys and self-certifications, malicious intermediate nodes would not be able to modify packets during the route discovery process. And this scheme uses nonce and timestamp to prevent from replay attack.

B. Passive attacks:

In passive attacks, an intruder snoops the data exchanged without altering it. The attacker mainly eavesdrop the data packets in the network without doing any active operations, or just refuse to execute the requested function. The goal of the attacker is to obtain information that is being transmitted, thus violating the message confidentiality. Since the activity of the network is not disrupted, these attackers are difficult to detect.

In this scheme, source node and destination node use their public key and session key to encrypt the communication data between them. Since the important information is encrypted during route discovery process, passive attackers cannot access the message without the knowledge of corresponding keys. Moreover, the use of an information dispersal technique makes difficult for passive attackers to get whole information.

7. Performance Evaluation

In order to evaluate the performance of the proposed framework in wireless ad hoc network, we have designed experimental model and simulated using OPNET Modeler (Opnet, 2008). We have modified DSR model to provide multipath routing protocols as per proposed framework.

7.1 Simulation Environment

In the simulation, the network coverage area is a 1000m x 1000m square with 50 mobile nodes, each having radio power range of 300m. The channel capacity is 2 Mbps. The IEEE 802.11 Distributed Coordination Function (DCF) is used as the MAC-layer protocol. The nodes are initially uniformly distributed throughout the network area and their movement is determined by the random waypoint mobility model. We have used a pause time of 1.0s for all the experiments. The speed of the nodes varies from 0m/s to 20m/s.
The traffic model of the audio streaming system considered employs G.729 codec for which the payload is 10 bytes and packet rate is 50 packets per second. Two simulatenous streamings can occur and the sources and destinations are chosen randomly with uniform probabilities. Each run executes 300 seconds of simulation time.

7.2 Simulation Scenarios and Metrics

For the simulation, two scenarios have been designed in wireless ad hoc environment - benign environment and adverse environment.
Under normal condition, we assume that there is no misbehaving nodes along the paths. And all the intermediate nodes are good behaving. Whereas, a second one is under adverse environment, there may be individual misbehaving nodes that can cause black hole attack. This attack is a selective data forwarding attack, in which adversaries only forward routing control packets, while dropping all data packets.
Several simulations were carried out with three schemes, namely, the proposed scheme, single-path DSR, and Mao's scheme with layered coding and selective Automatic repeat-request (ARQ) in both the environments.
While simulating audio streaming in wireless ad hoc network in above mentioned environments, we have considered following three key performance metrics to be evaluated:

- Packet Delivery Ratio (PDR): This is the ratio of the number of data packet successfully delivered to the destinations to the number of data packets generated by the constant bit rate (CBR) sources. It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ratio, the more complete and correct is the routing protocol.
- Average end-to-end delay: The end-to-end delay, network delay, indicates how long it took for a packet successfully delivery from the CBR source to the application layer of the destination. It represents the average data delay in the network.
- Normalized routing load: It is measured by the number of routing control packets transmitted per data packet delivered at the receiver. This is an important metric to compare the performance of different protocols since it can give a measure of the efficiency of protocols, especially in a low bandwidth and congested wireless environment.

7.3 Results and Analysis

In the simulation, we have examined the performance of the proposed secure scheme under normal and adverse environments.

Under normal condition, the single-path DSR, Mao's scheme (Mao et al., 2005) with layered coding and selective ARQ and the proposed scheme are compared. The speed of node is varied from 0 m/s to 20 m/s.

Fig. 4 shows the packet delivery rate plotted against node speed for the single path DSR, Mao's scheme and the proposed framework. It can be seen that the packet delivery rate of the proposed scheme is less than that of the single path DSR and Mao's scheme. Whereas Mao's scheme has the highest PDR for all the node speed.

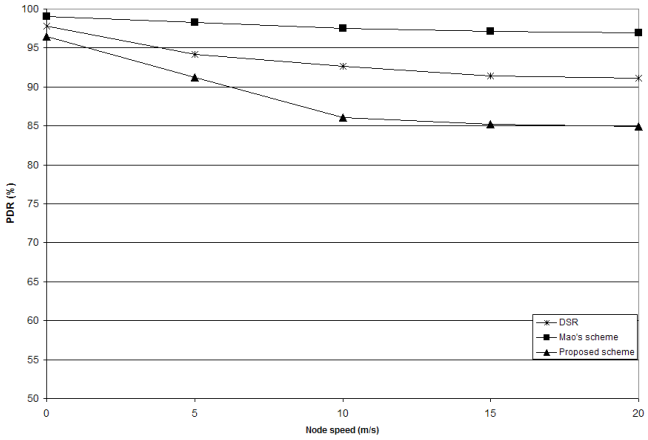

Fig. 4. Packet delivery ratio in normal environment

Fig. 5 shows the average end-to-end delay plotted against node speed for the single-path DSR, Mao's scheme and the proposed framework under normal condition. Due to cryptographic functions, the average delay of the proposed scheme is higher than that of the single path DSR and Mao's scheme. And it can be seen that Mao's scheme has the lowest average delay.

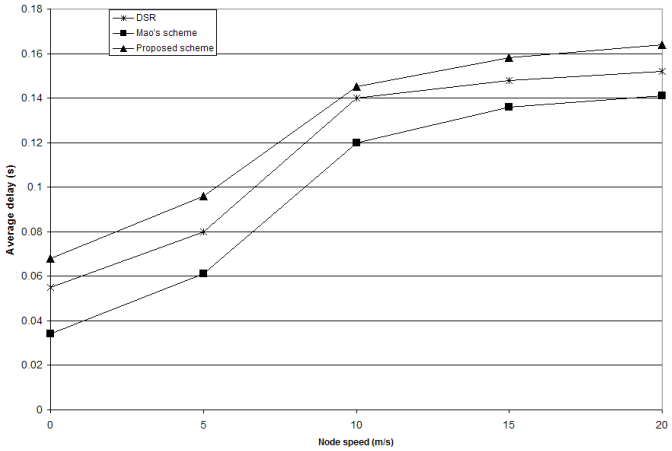

Fig. 5. Average end-to-end delay in normal environment

Fig. 6 shows the normalized routing load characteristics for single-path DSR, for Mao's scheme and proposed scheme. It can be seen that the normalized routing loads in Mao's scheme and the proposed scheme are much lower than that of DSR. With the increase of node speed, the normalized routing load in DSR increases more quickly than those in Mao's scheme and the proposed scheme. For two later schemes, it increases slowly with the increase of node speed. Since Mao's scheme and the proposed scheme can find multiple alternate route paths in a route discovery process, the protocols tremendously decrease the number of route rediscovery process. Whereas, since DSR encounters more link failures with the increase in mobility, it has to trigger more new route discovery process which causes more routing control packets.

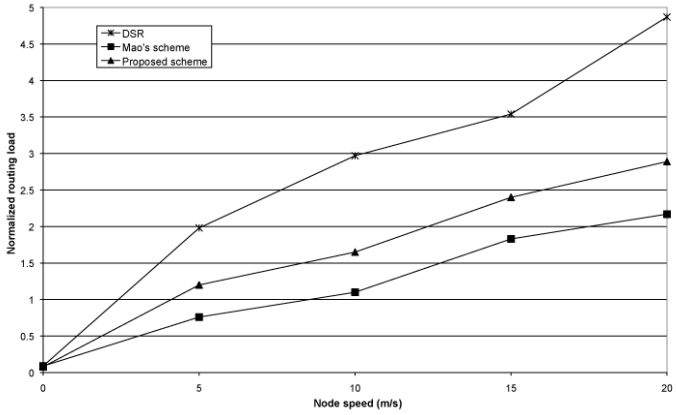

Fig. 6. Normalized routing load in normal environment

Under adverse environment, the proposed secure scheme is compared with the single-path DSR and Mao's scheme. The speed of node is at 10 m/s. And the percentage of misbehaving nodes in the network is varied from 0 to 20%.

Fig. 7 shows packet delivery rate plotted against number of misbehaving nodes for single-path DSR, Mao's scheme and the proposed secure framework. It can be seen that the packet delivery rate in network suffering different percentage of misbehaving nodes.

With the increase of misbehaving nodes in network, the packet delivery rate for the single DSR and Mao's scheme decrease dramatically. In case of the proposed secure scheme it is affected in a much lesser extent.

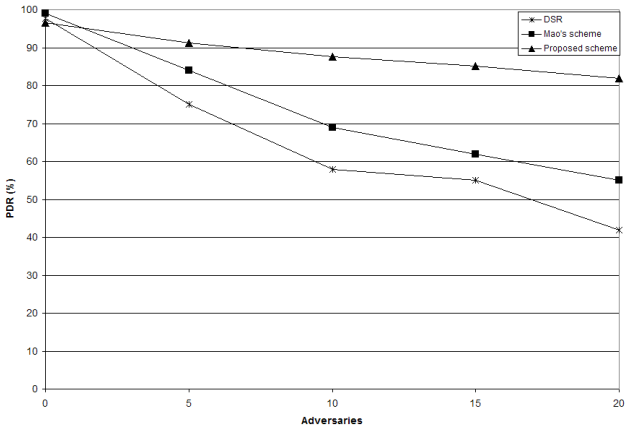

Fig. 7. Packet delivery ratio (adverse environment)

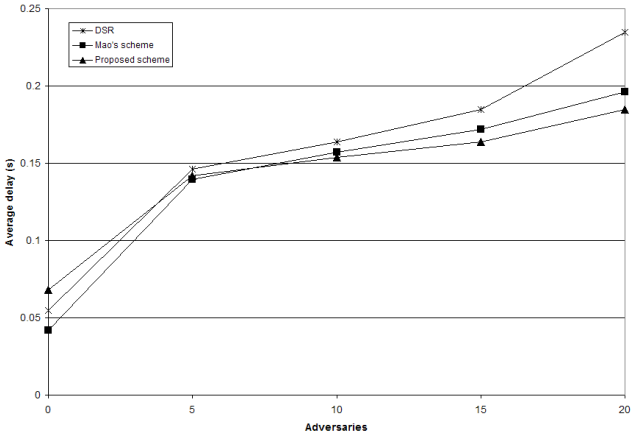

Fig. 8. Average end-to-end delay (adverse environment)

Fig. 8 shows average delay plotted against number of misbehaving nodes for single-path DSR, Mao's scheme and the proposed secure framework. It can be seen that the average delay in network increase with the increase in percentage of misbehaving nodes. At higher

percentage of malicious nodes, the average delay for the proposed scheme is lesser than single-path DSR, and Mao's scheme. With the increase of misbehaving nodes in network, the average delay for the single-path DSR increase significantly while that for Mao's scheme and proposed secure scheme increase steady.
Fig. 9 shows normalized routing load plotted against number of misbehaving nodes for single-path DSR, Mao's scheme and the proposed secure framework. It can be seen that the normalized routing loads for the single-path DSR, and Mao's scheme increase dramatically with increase of misbehaving nodes in network. Whereas, the normalized routing load for the proposed scheme is increased gradually.

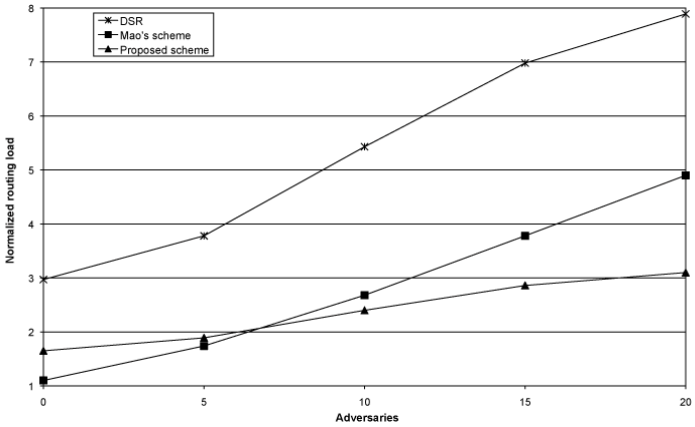

Fig. 9. Normalized routing load (adverse environment)

8. Conclusions

This chapter presents a secure and reliable framework for multipath audio streaming over wireless multihop network. It also shows the need of secure multipath routing protocol for multimedia streaming over wireless ad hoc network. While designing multipath routing scheme for a wireless ad hoc network, we have considered not only self-certified public keying technique and self-certificate but also digital signature and encryption technique for securing ad hoc routing as well as real-time data transfer. And we have considered Information Dispersal algorithm (IDA) in order to transmit real-time data through multiple paths. We have conducted security analysis for the proposed scheme and shown its robustness to various attacks. On implementing the proposed scheme in OPNET simulation, we have obtained various simulation results, which show that the performance of the proposed framework is better than the existing schemes under the adverse environment.
We can implement this scheme for video communication over multipath ad hoc network. Future work should consider on not only multipath but also multicast video streaming since multicast is an appealing technique for many applications, such as group video conferencing and video-on demand (VOD) services, and results in bandwidth savings as compared to multiple unicast sessions. We can also consider multiple video sources providing simultaneously service for multiple receivers.

9. Acknowledgements

This research was supported by the Plant Technology Advancement Program (07SeaHeroB01-03) funded by Ministry of Construction & Transportation, and the WCU Program (R31-2008-000-10026-0) by the Ministry of Education, Science, and Technology of Korean Government.

10. References

Berton, S.; Yin, H., Lin, C., & Min, G. (2006). Secure, Disjoint, Multipath Source Routing Protocol (SDMSR) for Mobile Ad-Hoc Networks, *Proceedings of Fifth International Conference on Grid and Cooperative Computing (GCC '06)*, pp 387--394, Oct. 2006

Girault, M. (1991). Self-certified public keys, *Proceedings of Advances in Cryptology (Eurocrypt'91)*, Springer, pp. 490-497, 1991

Hsieh, M. Y.; Huang, Y. M., & Chiang, T. C. (2007) Transmission of layered video streaming via multi-path on ad hoc networks, *Springer Multimedia Tools Applications*, Vol. 34, No. 2, 2007, pp. 155-177

Hu, Y. C.; Perrig, A., & Johnson, D. B. (2005) Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks, *Springer Wireless Network*, Vol. 11, No. 1-2, 2005, pp. 21-38

Johnson, D. B.; Maltz, D. A. & Broch, J. (2001). DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks, In: *Ad Hoc Networking*, C. E. Perkins (Ed.), Chapter 5, pp. 139-172, Addison-Wesley

Lee, B. & Kim, K. (2000). Self-certificate: PKI using self-certified key, *Proceedings of Conference on Information Security and Cryptology (CISC 2000)*, Vol. 10, No. 1 pp 65-73, 2000.

Lee, S. J. & Gerla, M. (2000). AODV-BR: Backup Routing in Ad hoc Networks, *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC 2000)*, Vol. 3, pp. 1311–1316, September 2000, IEEE

Lee, S. J. & Gerla, M. (2001). Split multipath routing with maximally disjoint paths in ad hoc networks, *Proceedings of IEEE International Conference on Communications (ICC'01)*, Vol. 3, pp. 867-871, Helsinki, Finland, 2001, IEEE.

Leung, R.; Liu, J., Poon, E., Chan, A., & Li, B. (2001). MP-DSR: A QoS-Aware Multi-Path Dynamic Source Routing Protocol for Wireless Ad-Hoc Networks, *Proceedings of 26th IEEE Annual Conference on Local Computer Networks (LCN 2001)*, pp. 132-141, November, 2001

Lou, W.; Liu, W., Zhang, Y., & Fan, Y. (2009). SPREAD: Improving network security by multipath routing in mobile ad hoc networks. *Springer Wireless Networks*, Vol. 15, No. 3, 2009, pp. 279-294

Mao, S.; Lin, S., Panwar, S. S., Wang, Y., & Celebi, E. (2003). Video transport over ad hoc networks: multistream coding with multipath transport. *IEEE Journal on Selected Areas in Communications*, Vol. 21, No. 10, 2003, pp. 1721-1737

Mao, S.; Lin, S., Wang, Y., Panwar, S.S., & Li, Y. (2005). Multipath video transport over ad hoc networks. *IEEE Wireless Communications*, Vol. 12 No. 4, pp. 42-49, Aug. 2005

Marina, M. K. & Das, S. R. (2006). Ad hoc on-demand multipath distance vector routing. *Wiley Wireless Communications and Mobile Computing*, Vol. 6, No. 7, pp. 969–988, 2006

Marshall, J.; Thakur, V., & Yasinsac, A. (2003). Identifying Flaws in the Secure Routing Protocol, *Proceedings of 22nd International Performance, Computing, and Communications Conference (IPCCC 2003)*, Phoenix, Arizona, USA, April 9-11, 2003, pp. 167-174.

Mavropodi, R.; Kotzanikolaoua, P., & Douligerisa, C. (2007). SecMR- a secure multipath routing protocol for ad hoc networks, *Elsevier Ad Hoc Networks*, Vol. 5, Issue 1, January 2007, pp 87-99

Mishra, A. *Security and Quality of Service in Ad hoc Wireless Networks*, Cambridge University Press, 2008

Mohapatra, P. & Krishnamurthy, S. (2004). *Ad Hoc Networks: technologies and protocols*. Springer Science & Business Media, Inc., 2004

Mueller, S.; Tsang, R. P. & Ghosal, D. (2004). Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges, In: *Performance Tools and Applications to Networked Systems*, LNCS 2965, pp. 209-234

OPNET Modeler, URL: http://www.opnet.com. Accessed on July 2008

Papadimitratos, P. & Haas, Z. J. (2002). Secure Routing for Mobile Ad hoc Networks, *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, San Antonio, TX, USA, 2002

Papadimitratos, P. & Haas, Z. J. (2006). Secure Data Communication in Mobile Ad hoc Networks. *IEEE Journal on Selected Areas in Communications*, Vol. 24, No. 2, 2006, pp. 343-356

Perkins, C. E.; Belding-Royer, E., & Das, S.R. (2003). Ad hoc on-demand distance vector (AODV) routing. *IETF RFC 3561,* July 2003

Pervaiz, M. O.; Cardei, M., & Wu, J. (2007). Routing Security in Ad Hoc Wireless Networks, *Network Security*, S. Huang, D. MacCallum, & D. Z. Du (Eds.), 2007 Springer

Rabin, M. O. (1989). Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal of the ACM*. Vol. 36, No. 2, pp 335-348, 1989

Sanzgiri, K.; LaFlamme, D., Dahill, B., Levine. B.N., Shields, C., & Belding-Royer, E.M. (2005) Authenticated Routing for Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*, Vol. 23, No. 3, 2005, 598–610

Wang, L.; Shu, Y., Dong, M., Zhang, L., & Yang, O. W. W. (2001). Adaptive Multipath Source Routing in Ad Hoc Networks, *Proceedings of IEEE International Conference on Communications (ICC 2001)*, Vol. 3, pp. 867-871, Helsinki, Finland, June 2001

Wang, L.; Shu, Y., Zhao, Z., Zhang, L., & Yang, O. W. W. (2002). Load Balancing of Multipath Source Routing in Ad Hoc Networks, *Proceedings of IEEE International Conference on Communications (ICC 2002)*, Vol. 5, pp. 3197-3201, 2002

Wei, W. & Zakhor, A. (2004). Robust Multipath Source Routing Protocol (RMPSR) for Video Communication over Wireless Ad Hoc Networks, *Proceedings of IEEE International Conference on Multimedia and Expo (ICME 2004)*, Vol. 2, pp. 1379-1382, Taiwan, June 2004

Ye, Z.; Krishnamurthy, S.V., & Tripathi, S.K. (2004). A routing framework for providing robustness to node failures in mobile ad hoc networks. *Elsevier Ad Hoc Networks Journal*, Vol. 2, No. 1, 2004, pp. 87–107

Zhou, L. & Haas, Z. J. (1999) Securing ad hoc networks, *IEEE Network*, Vol. 13, No. 6, pp. 24–30, 1999