# A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET

**S.Dhanalakshmi**
Senior Lecturer , Department of Computer Applications
Dr.Mahalingam College of Engineering and Technology,
Anna University, Coimbatore, Tamil Nadu, India

**Dr.M.Rajaram**
Assistant Professor & HOD of EEE
Thanthai Periyar Govt. Institute of Technology
Vellore, Tamil Nadu, India

**Summary**
For the protection of both routing and data forwarding operations, a network layer security solution has been provided as a solution for various security attacks in ad hoc networks. In this paper, to develop a security framework has been proposed. This security framework involves: Detection of malicious nodes by the destination node, isolation of malicious nodes by discarding the path and prevention data packets by using dispersion techniques. Our Reliable and Secure Framework (RSF) consists of a Reliable Multipath Routing (RMR) algorithm, which determines a set of node-disjoint reliable paths. The paths are arranged in the descending order of their reliability index. Data packets are dispersed and transmitted simultaneously through the reliable disjoint paths. The primary reliable path sends the information packet containing the transmission information. At the destination, if there is mismatch between the transmission information and the data packets received, a negative feedback is sent back to the source that includes the particulars of the affected paths. The affected paths are then removed from the list of node-disjoint paths by the source. The destination can recover the data effectively by attaining reliability, since the data packets are dispersed along multiple paths usaing an efficient dispersion algorithm.

Our simulation results shows that, when compared with existing scheme, our framework reduces overhead and delay, at the same time increasing the packet delivery ratio.

***Key words:***
*Detection, Multipath, Reliable, Dispersion, Malicious*

## 1. Introduction

A mobile ad-hoc network (MANET) is a transitory infrastructure less multi-hop wireless network wherein the nodes can move randomly. With multi-hop packet forwarding, the limited wireless transmission range of each node has been extended by such networks. Therefore, they become compatible for the scenarios wherein pre-deployed infrastructure support is not available. No static infrastructure for instance base stations or mobile switching centers present in an ad hoc network. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Frequent changes of the network topology have been caused by the node mobility in an ad hoc network.

The research actions concerning security in MANETs are still at their initiation, whereas the routing aspects of MANETs are previously well understood. In addition to the problems of regular networks, MANETs face a number of new security problems.

The malicious nodes can readily function without proper security, as routers and prevent the network from delivering the packets properly. For example, the malicious nodes can declare incorrect routing updates. Subsequently they are propagated in the network or drop all the packets passing through them. Thus security issue in ad hoc networks, specifically the protection of their network-layer operations from malicious attacks, is extremely important.

On distributed computer systems, there are a number of well-known attacks. These include

- Denial of Service: A network service is not available due to overload or malfunction.
- Information theft: Information is read by an unauthorized instance.
- Intrusion: Access to some restricted service is gained by an unauthorized person.
- Tampering: Data is modified by an unauthorized person.

As a solution for these kind of attacks, a network layer security solution has been provided in ad hoc networks. In this paper, developing a security framework has been proposed. This security framework involves:

1. Detection of malicious nodes by the destination node.
2. Isolation of malicious nodes by discarding the path.
3. Prevention data packets by using dispersion techniques

Manuscript received October 5, 2008
Manuscript revised October 20, 2008

Our Reliable and Secure Framework (RSF) consists of a Reliable Multipath Routing (RMR) algorithm, which determines a set of node-disjoint reliable paths. The paths are arranged in the descending order of their reliability index. Data packets are dispersed and transmitted simultaneously through the disjoint multiple paths. The information packet is sent through the primary reliable path. At the destination, if there is mismatch between the transmission information and the data packets received, a negative feedback is sent back to the source which contains the details of the affected paths. The source now discard the affected paths from the list of node-disjoint paths. Since the data packets are dispersed along multiple paths using an effective dispersion algorithm, the destination can recover the data successfully.

The paper is organized as follows. Section 2 discusses the related work done in the same area. Section 3 presents the possible misbehaviors on data. Section 4 describes our proposed RSF framework. Performance Evaluation and simulation results are given in section 5 and the conclusion is given in section 6.

## 2. Related Work

An intrusion detection in wireless networks has been proposed by Farooq Anjum et al. [1]. The intrusion detection community has been focused primarily on wired networks. A relationship among the likelihood of detecting an intrusion and the amount of nodes that must take part in the process of detecting intrusions has been probed by them. Activities on the networks have been observed and compared with known attacks by signature-based IDS. On the other hand, new unidentified threats cannot be detected in this approach. This is the main disadvantage of this approach.

Based on AODV over IPv6, a proof-of-concept implementation of a secure routing protocol has been proposed by Anand Patwardhan et al. [2] and a routing protocol-independent Intrusion Detection and Response system for ad-hoc networks strengthens this further. However, the routing attacks only principally conversed in the techniques presented in this paper.

For MANETs with formal reasoning and simulation experiments for evaluation, CHIN-YANG and HENRY TSENG [3] proposed a absolute distributed intrusion detection system includes four models. However this too converse only the routing attacks not the others.

The detection phase has been focused by Tarag Fahad and Robert Askwith [4] and offered a new mechanism utilized to detect selfish nodes in MANET. Packet Conservation Monitoring Algorithm (PCMA) is the latest detection mechanism. The issue of packet forwarding attacks only has addressed by this mechanism not the further threats.

The secure message transmission (SMT) protocol and its alternative, the secure single-path (SSP) protocol have been presented by Panagiotis Papadimitratos,and Zygmunt J. Haas [5],[14]. A route discovery protocol was proposed in [12]. In [13] proposed a Secure Link State Routing Protocol (SLSP). This Secure Link State Routing Protocol (SLSP) gives safe proactive topology discovery that can proliferate advantageous to the network operation. Misbehaviors cannot be detected in this method, while reliability is attained.

To stimulate cooperation among mobile nodes with individual interests, a credit-based Secure Incentive Protocol (SIP) has been proposed by Yanchao Zhang et al. [7]. The competence of SIP has been recognized through the thorough simulation studies. The issue of packet forwarding attacks has been addressed in this, not the other threats.

To notice routing misbehavior and to alleviate their unfavorable effect, the 2ACK scheme that serves as an add-on technique for routing schemes has been recommended by Liu [8]. Sending two-hop acknowledgment packets in the contradictory direction of the routing path is the major thought of the 2ACK scheme. Even if there is no misbehavior, the acknowledgement packets are sent. This results in pointless overhead.

To mitigate adverse effects of misbehavior, a Multipath Routing Single path transmission (MARS) scheme has been proposed and improved by Li Zhao et al. [9]. With uninterrupted feedback mechanism, it merges multipath routing and single path data transmission. However, the information packets are disallowed from attaining the destination by a route failure or link failure. Furthermore, the destination may not be competent to detect the misbehavior, if a selfish node does not forward the information packet or adjusts the contents of the information packet.

An mIDS (Mobile Intrusion Detection System) appropriate for multi-hop ad-hoc wireless networks has been proposed by S.Madhavi and Dr. Tai Hoon Kim [11]. This detects nodes' misbehavior and abnormalities in packet forwarding such as intermediate nodes dropping or delaying packets.

## 3. Misbehavior on Data

Different types of misbehavior out of different purposes have been created by the misbehaving nodes in an ad hoc network. The types of misbehavior on data related to the work are discussed here.

### 3.1. Data Dropping

This is the denial of service (DoS) attack. In this attack, the selfish or malicious intermediate nodes decline to forward data packets for other nodes in the network. In this paper two adverse environments are inspected. They represent the types of data dropping misbehavior formed by individual and cooperating misbehaving nodes respectively.

*A. Individual dropping:* This is a relatively simple type of misbehavior. The misbehaving nodes drop all or a certain percent of the received data packets because of unlike intentions. Most schemes [18], [19], [20] detecting misbehavior on data have expected to deal with this kind of misbehavior.

*B. Colluded dropping:* This is an advanced type of misbehavior formed by two cooperating malicious nodes. It is difficult to detect and defend this attack. It is assumed that two malicious intermediate nodes N1 and N2 are connected on a data transmission path. N1 forwards received data packets to N2, and N2 drops all or part of them. N1 tries to cover the data droppings at N2 by ignoring it and/or generating / forwarding faked acknowledgements in the system. As N1 would not report the misbehavior of N2 to the system, the overhearing schemes [18], [19] fail to detect such colluded misbehavior. Since N1 could forward faked 2ACK generated by N2 or generate faked 2ACK for N2, neither of the protocols proposed in [20] could detect such fabricated packets and this colluded dropping. The schemes discussed in [21], [22] tackle such colluded misbehavior

### 3.2. Data Modifying

During their transmission, the malicious nodes alter the received data packets. One malicious node is assumed to form the data modifying misbehavior independently along the data transmission path. Whereas the schemes in [21], [22] can successfully detect such misbehavior, the schemes in [19], [20] cannot detect such kind of misbehavior.

## 4. System Components

### 4.1. Determination of the Multi Path Set (MPS) by RMR

Our routing protocol RMR uses an Multi Path Set (MPS) comprising node-disjoint paths, determined using the AOMDV protocol [15]. An MPS of node-disjoint paths is constructed by successively calculating the node-disjoint, shortest in number of hops, paths, using the network connectivity information provided by the route discovery.

Since an adversary “tactically” positioned on the overlap segment of two or more incompletely disjoint routes would control communication across those routes, node disjointness enhances the robustness of RMR. However, it is probable the protocol operates in conditions to allow just a few node-disjoint paths to be discovered, for example, because of low-connectivity network topology or disturbance of the route discovery by opponents.

The number of paths RMR should operate depends on the protocol’s configuration objective, or it can be a protocol-selectable parameter. While new connectivity information is obtained, RMR attempts to determine new paths usually either proactively or reactively, following the invocation of a route discovery.

Conversely, to avoid repeated invocations at what time no extra paths can be discovered, route discoveries aspiring to enhance the MPS must be rate-limited. Finally, we note that placing the route selection at the sender implies that data are source-routed, functionality that is easy to combine with existing secure routing protocols.

#### 4.1.1 Determining Reliability Index for RMR

Many node misbehaviors have been proactively protected by robust information dispersion and multi-path data forwarding, particularly when misbehaving nodes are low. Conversely, a closed loop feedback system is proposed to respond to these behaviors based on Reliability Index (PRI) of the paths to defy against time changeable misbehaviors, blinking link accessibility, network congestion and most significantly misbehaving nodes high. Therefore, our proposed mechanism is able to tune itself for the best performance in each situation.

In terms of reliability, RI reflects the status of the paths. This will be utilized to choose the active paths in the subsequent transmission and the way they will be loaded. Consistent with the performance of the path in terms of packet delivery ratio, R1 is measured at the destination as

$$RI_k = Pd_k * W$$

Where $RI_k$ is the reliability index of the kth path and $Pd_k$ is the packet delivery ratio of the kth path.

By tracking the behavior of the paths through running a closed loop feed-back mechanism derived from RI, RMR will try to dynamically maximize packet delivery ratio. RI is delivered to the source by the acknowledgment packets sent through multiple paths, since it is measured at destination and used at source.

### 4.2 Prevention of Data by Using Dispersion Technique

After the determining MPS, the source *S* disperses each outgoing message, adding restricted redundancy to the

data and separating the resultant information into pieces that are transmitted across the MPS routes one piece per route. When M out of N pieces are received successfully, the message can be reconstructed at the destination, even if some of the pieces are lost or corrupted. The ratio $r = N/M$ is termed the redundancy factor, and we denote a dispersed message with redundancy $r$ as an $(M, N)$-message

A message authentication code (MAC), measured with $K_{S,T}$, and a sequence number are attached to each piece, so that *T* can validate their integrity and origin authenticity, and decline replayed traffic. Through cryptographically protected and dispersed feedback, *T* reports successfully received pieces back to *S*. *S* validates the feedback messages, unless a retransmission timer (RTO) expires when none of the message or feedback pieces are received.

The rating of the MPS routes are continuously updated during the transmission across the MPS. The rating of the corresponding route is increased or decreased depending on the success or failure of the piece. To be efficient in high attacking scenarios, the protocol adjusts its configuration by continuously monitoring the quality of the used paths and collecting statistical information on the network through trusted feedback. In case the dispersed message cannot be reconstructed, *T* waits for *S* to retransmit the missing pieces $\mathrm{Retry}_{\mathrm{MAX}}$ times, per services message. Here $\mathrm{Retry}_{\mathrm{MAX}}$ is a protocol-selectable maximum number of retransmissions. Details and an example of the dispersion algorithm [16], which acts in essence as an erasure code, are given in [17].

## 4.3 Detection and Removal of Malicious Nodes by the Destination

The scheme can efficiently detect the types of misbehavior on data discussed in Section 3. Here, the misbehaving nodes are assumed to manipulate the transmitted data but forward the control packets.

### 4.3.1 New Control Packets

Our scheme tackles misbehavior through the use of two new types of control packets, termed PI and NACK. A PI (packet information) packet, used to detect misbehavior, is sent from the source to the destination at the start of data transmission. A NACK packet, used to mitigate the adverse effects, is sent from the destination to the source when suspected misbehavior along data transmission path is detected.

A PI packet contains information of the corresponding transmission: (a) data generation information such as data generation rates, data packet size, and expected data amount; (b) data transmission path information, including the path length and nodes along the path. A PI packet can also carry a randomly generated key to authenticate the data packets of the corresponding transmission batch.

A NACK packet contains an alert identifier and information of path pair, including lengths of paths and nodes along paths.

### 4.3.2 Packet Authentication

It is assumed that a security association (SAs, d), such as a symmetric shared key, between the source and the destination exists in the framework. Since two nodes choose to employ a secure communication scheme, their ability to authenticate each other is indispensable.

Each of the data and control packets in the system carries a message authentication code (MAC) calculated from the source and destination IDs and the (SAs, d). As a result, the end nodes can verify the integrity and the authenticity of these packets, whose structures are shown in Fig. 1.

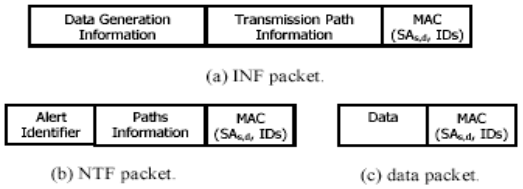


Fig. 1. Structure of different packets for security transmission.

### 4.3.3 Misbehavior Detection at Destination

In the proposed framework, the source gets the primary reliable path R1 from the MPS before sending out data packets. Out of the n disjoint reliable paths (Rn) from the MPS, data packets are dispersed and transmitted through m reliable paths (Rm). To help the destination monitor the performance of dispersed routes Rm used for data transmission, a PI packet is sent through R1 right after the data packets has been sent to Rm. The PI packet contain the information of this transmission.

To detect misbehavior, a table called Path Table (PT) as shown in Fig. 2, is maintained at the destination.

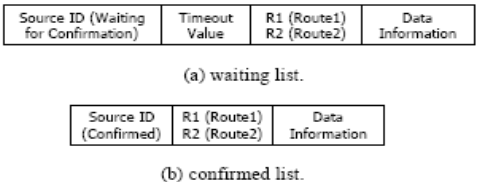


Fig.2. Table kept in destination for misbehavior detection.

Upon receiving a packet containing new transmission information from source, the destination puts the source ID, a timeout value t, and the transmission information into the

PT. After the source ID and corresponding information has been moved into the PT, the destination keeps a value *S* to record the number of received data packets during each observation time *T*. At the end of each observation time, the destination compares the statistic value *S/T* with the data rate value in the data information saved in the PT. When it detects the data dropping or data modifying misbehavior, the destination sends a NACK packet back to source through R1 and removes the source ID and corresponding items from the table.

If all data packets are dropped by misbehaving nodes along Rm individually or collaboratively, the destination would not receive the data packet with matched transmission information within the timeout limit. The misbehavior is then detected. If the data packets are partly discarded to a certain extent, the difference between the statistic value S/T, which is obtained after an observation period T, and the data rate value, which is delivered by PI packet and saved in the PT, would exceed a specified limitation.

Hence, from the information saved in the PT, such misbehavior would still be detected. If the data packets are modified during transmission, the destination would detect this through calculating the message authentication code (MAC) in the data packets.

4.3.4 Removal of Misbehavior Nodes

Upon receiving a NACK packet, the source removes the corresponding paths from its MPS and route cache. If it still has data to send, the source checks the MPS for the next k reliable node disjoint paths (Rk) and sends the dispersed data packets and PI, containing new transmission information. The source initiates a route request procedure if no node-disjoint paths are available in the MPS. The destination removes the corresponding items from the table when it receives a RREQ from source, and updates the table when it receives packets containing new information.

If new transmission information is received after the previous information of the source has been confirmed, the destination updates the corresponding item from the PT. The destination removes the corresponding items from the PT when it receives a new RREQ from a source.

## 5. Performance Evaluation

### 5.1 Simulation Model and Parameters

We use NS2 to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage.

In our simulation, mobile 50 mobile nodes move in a 1000 meter x 1000 meter rectangular region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 250 meters. In this mobility model, a node randomly selects a destination from the physical terrain. It moves in the direction of the destination in a speed uniformly chosen between the minimal speed and maximal speed. After it reaches its destination, the node stays there for a pause time and then moves again. In our simulation, the minimal speed is 5 m/s and maximal speed is 10 m/s. The simulated traffic is Constant Bit Rate (CBR). We vary the no. of misbehaving nodes as 5, 10, 15 and 20.

Our simulation settings and parameters are summarized in table 1

| | |
|---|---|
| No. of Nodes | 50 |
| Area Size | 1000 X 1000 |
| Mac | 802.11 |
| Radio Range | 250m |
| Simulation Time | 50 sec |
| Traffic Source | CBR |
| Packet Size | 512 |
| Speed | 5m/s t 10m/s |
| Misbehaving Nodes | 5,10,15 and 20 |

### 5.2 Performance Metrics

We compare RSF with the SMT [5] scheme**.** We evaluate mainly the performance according to the following metrics.

**Control overhead:** The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets.

**Average end-to-end delay:** The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

**Average Packet Delivery Ratio:** It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

The simulation results are presented in the next section.

### 5.3 Results

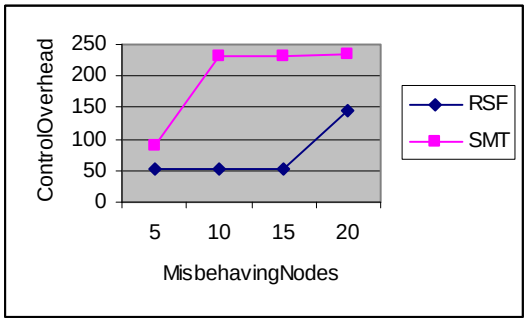


Fig3.Control Overhead of Misbehaving Nodes

Fig. 3 shows the results of Control overhead for the misbehaving nodes 5, 10….20. From the results, we can see that RSF scheme outperforms the SMT scheme by attaining low overhead.

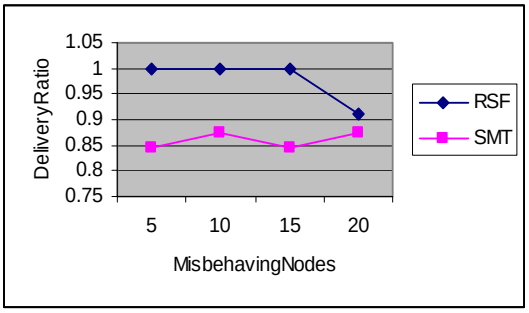


Fig4.Delivery Ratio of Misbehaving Nodes

Fig.4 shows the results of average packet delivery ratio for the misbehaving nodes 5, 10….20. Clearly our RSF scheme achieves more delivery ratio than the SMT scheme since it has both reliability and security features.

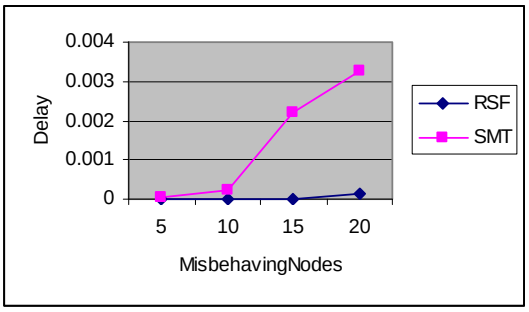


Fig5.End-to-End Delay of Misbehaving Nodes

Fig. 5 shows the results of average end-to-end delay for the misbehaving nodes 5, 10….20. From the results, we can see that RSF scheme outperforms the SMT scheme by attaining low delay.

## 6. Conclusion

In this paper, we develop a security framework which involves: Detection of malicious nodes by the destination node, isolation of malicious nodes by discarding the path and prevention data packets by using dispersion techniques. Our Reliable and Secure Framework (RSF) consists of a Reliable Multipath Routing (RMR) algorithm, which determines a set of node-disjoint reliable paths. The paths are arranged in the descending order of their reliability index. Probe data packets are dispersed and transmitted simultaneously through the reliable disjoint paths. The information packet containing the transmission information is sent through the primary reliable path. At the destination, if there is mismatch between the transmission information and the data packets received, a negative feedback is sent back to the source which contains the details of the affected paths. The source now discard the affected paths from the list of node-disjoint paths. Since the data packets are dispersed along multiple paths using an effective dispersion algorithm, the destination can recover the data successfully, there by achieving reliability. Our simulation results shows that, when compared with existing scheme, our framework reduces overhead and delay, at the same time increasing the packet delivery ratio.

## References

[1] Farooq Anjum and Dhanant Subhadrabandhu and Saswati Sarkar “Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols” Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th, Oct. 2003.

[2] Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis “Secure Routing and Intrusion Detection in Ad Hoc Networks” Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on March 2005.

[3] CHIN-YANG HENRY TSENG “Distributed Intrusion Detection Models for Mobile Ad Hoc Networks” University of California at Davis Davis, CA, USA , 2006.

[4] Tarag Fahad & Robert Askwith “A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks” The 7th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, 26-27 June 2006.

[5] Panagiotis Papadimitratos,and Zygmunt J. Haas “Secure Data Communication in Mobile Ad Hoc Networks” Ieee Journal On Selected Areas In Communications, Vol. 24, No. 2, February 2006.

[6] Ernesto Jiménez Caballero “Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem” 2006.

[7] Yanchao Zhang, Wenjing Lou, Wei Liu, and Yuguang Fang, "A secure incentive protocol for mobile ad hoc networks", *Wireless Networks (WINET)*, vol 13, issue 5, October 2007.
[8] Liu, Kejun Deng, Jing Varshney, Pramod K.Balakrishnan, Kashyap "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs" Mobile Computing, IEEE Transactions on May 2007.
[9] Li Zhao and José G. Delgado-Frias "MARS: Misbehavior Detection in Ad Hoc Networks" Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE Publication Date: 26-30 Nov. 2007.
[10] A.Patwardhan, J.Parker, M.Iorga, A. Joshi, T.Karygiannis and Y.Yesha "Threshold based Intrusion Detection in Adhoc Networks and Secure AODV" Elsevier Science Publishers B. V., Ad Hoc Networks Journal (ADHOCNET), June 2008.
[11] S.Madhavi and Dr. Tai Hoon Kim "AN INTRUSION DETECTION SYSTEM IN MOBILE ADHOC networks" International Journal of Security and Its Applications Vol. 2, No.3, July, 2008.
[12] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks" in Proc. SCS CNDS, San Antonio, TX, Jan. 27–31, 2002, pp. 193–204.
[13] P. Papadimitratos and Z. J. Haas, "Secure link state routing for mobile ad hoc networks," in Proc. IEEE CS Workshop on Security and Assurance in ad hoc Network, Orlando, FL, Jan. 2003, pp. 379–383.
[14] P. Papadimitratos and Z.J. Haas, "Secure Message Transmission in Mobile Ad Hoc Networks," ACM MobiCom Workshop on Wireless Security (WiSe), San Diego, CA, September 2003
[15] Mahesh K.Marina and Samir R.Das, "Ad hoc On-demand Multipath Distance Vector Routing", IEEE 2001.
[16] M. O. Rabin, "Efficient dispersal of information for security, load balancing, and fault tolerance," *J. ACM*, vol. 36, no. 2, pp. 335–348, Apr.1989.
[17] P. Papadimitratos and Z. J. Haas, "Secure message transmission in mobile ad hoc networks," *Elsevier Ad Hoc Netw. J.*, vol. 1, no. 1, pp. 193–209, Jul. 2003.
[18] S. Marti, T.J.Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," Proc. MobiCom 2000.
[19] K. Paul and D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks," Proc. GlobeCom 2002.
[20] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: preventing selfish in mobile ad hoc networks," Proc. WCNC'05, 2005.
[21] W. Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," IEEE INFOCOM 2004, pp. 2404 – 2413.
[22] K. Stewart, T. Haniotakis, and S. Tragoudas, "A security protocol for sensor networks," Proc. IEEE GlobeCom 2005.

**S.Dhanalakshmi** received B.Sc in Chemistry from Madras University, Madras in 1995 and Master of Computer Applications from Bharathidasan University, Tiruchirapalli in 1998 and M.Phil in Computer Science from Periyar University, Salem in 2004. Currently she is working as a Senior Lecturer at Department of Computer Applications, Dr.Mahalingam College of Engineering and Technology, Pollachi. Her areas of interests are Computer Networks and Mobile Communications.

**Dr. M.Rajaram** received B.E. in Electrical and Electronics Engineering from Madurai Kamaraj University, Madurai, in 1981, M.E in Power System Engineering from Bharathiyar University, Coimbatore in 1998 and Ph.D in the field of Control Systems from Bharathiyar University, Coimbatore, in 1993. Currently he is working as an Assistant Professor& Head of the Department of EEE, Thanthai Periyar Govt. Institute of Technology, Vellore. His areas of interests are Control Systems and Computer networks.