International Journal Of Scientific & Engineering Research, Volume 4, Issue 5, May-2013
ISSN 2229-5518

Risk-Aware Mechanism to Mitigate Routing Attacks in MANET by Distributed Node Control Method

A.Jaganraj (M.E), A.Yogaraj M.Tech, K.Aishwarya M.E

Abstract—The topological nature of MANET(Mobile Ad-hoc Network) itself demands high security due to its mobility movement, but designing a risk aware routing path for MANET is a complex task because of its Dynamic nature of Infrastructure. In this proposal, designing an Dynamic routing path decider to find less risk aware routing path for effective communication. The efficiency of the throughput and Routing failures can be further reduced by making Nodes of MANET to be more Knowledgeable, that is with more Metadata parameters. This paper introduce a class of metrics to measure the effective security offered in a wireless network as a function of the routing topology and the link security provided by the key assignment protocol. This joint protocol analysis allows a network analyst or an adversary to evaluate the vulnerability of network traffic and isolate weakly secured connections. Its show how an intelligent adversary can mount a node capture attack using vulnerability evaluation to focus the attack on the nodes which contribute maximally to the compromise of network traffic.

Keywords- Mobile Ad-hoc Network, Risk aware, Multilevel-data, Routing attack, Distributed node, Attack detection, Attack Mitigation.

1 Introduction

TO inspect the multilevel data packets even with compressed data. MANET Network is prone to highly vulnerable attacks due to its dynamic nature of Network infrastructure, among these Routing attacks received considerable attention since entire MANET structure will collapse on routing failures or router snooping. Existing methods will result in Node isolation which leads to unexpected network partition which may backfire rather than protecting. The studies on node capture attacks have all focused on the ability of an adversary to compromise the security of single-hop wireless links. However, messages in a wireless network traverse multiple links and paths between a source and destination node, and a message may be compromised by traversing a single insecure link. The overall security of routed messages is thus dependent on the routing protocol implemented in the wireless network, as well as the physical network topology and the relative positions of the source and destination nodes in the network.

Moreover, the fact that a message is transmitted over numerous links between a source and destination node implies that the overall confidentiality and integrity of the routed message may only be as secure as the least secure link, implying that vulnerabilities arise due to the topology of secure links in the wireless network.

Hence, the impact of a node capture attack is a function of both the cryptographic protocol which provides link security and the routing protocol which determines the set of links traversed by a given message. Mobile Ad hoc Network (MANET) are a class of wireless communication networks without a fixed infrastructure. the MANET concept basically evolved to tackle disaster situation like tsunami, earthquake, terrorist activities, battlefields, land-slides, etc. Later, the concept has been extended to include applications such as online education,gaming,business.

Several applications in MANETs need group communication to manage the situations. The MANET nodes do not provide reliable services and QoS (Quality of Service) guarantees as compared to other wireless networks such as WiFi, WiMAX, GSM and CDMA. The main sources of unreliability in MANETs are due to limited battery capacity, limited memory and processing power, varying channel conditions, less stability under unpredictable and high mobility of nodes. The QoS parameters to be guaranteed for multimedia group communication are bandwidth, delay, packet loss, jitters and bandwidth-delay product.

Ad hoc networks consist of hosts interconnected by routers without a fixed infrastructure and can be arranged dynamically. Considerable work has been done in the development of routing protocols in different types of ad hoc networks like MAN ETs, WMNs, WSNs, and VANETS etc [1]. In recent years, the interest in ad hoc networks has grown due to the availability of wireless communication devices that work in the ISM bands. While designing an ad hoc network in particular we are concerned with the capabilities and limitations that the physical layer imposes on the network performance. Since in wireless networks the radio communication links are unreliable so it is desirable to come up with an integrated design comprising of physical, MAC and network layers. The main vision of MANET is to support

- *Jaganraj A is currently pursuing masters degree program in computer science & engineering in Anna University,chennai ,India. PH-+919500922494. E-mail: jagan_math88@yahoo.co.in.*
- *Yogaraj A was completed master degree in Anna university and currently working as Assistant professor in Veltech University, Chennai, . E-mail: yoga.rajam@yahoo.co.in.*
- *Aishwarya K was finished master degree affiliated to Anna university & currently working as Assistant professor affiliated to Anna university college,India. E-mail: aishumecse@gmail.com.*

robust and efficient operation in wireless networks by incorporating routing functionalities at each mobile node. For such designing aspects of ad hoc networks Routing-based approach, Information-theoretic approach, Dynamic control approach or Game- theoretic approach has been implemented [2].

In MANET t o support mobile computing a mobile host must be able to communicate with other mobile hosts which may not lie within it' s radio transmission range. Hence routing protocols will need to perform four important functions as determination of network topology, maintaining network connectivity, transmission scheduling and channel assignment, and packet routing. Routing protocols in MANETs were developed based on the design goals of minimal control overhead, minimal processing overhead, multi hop routing capability, dynamic topology maintenance and loop prevention [3]. Classification on routing protocols in MANETs can be done on routing strategy wise or network structure wise.

According to routing strategy the routing protocols can be categorized as table- driven or proactive and source - initiated or reactive or on-demand routing. Each of these types of protocols behaves differently on different wireless conditions. Hence the performance analysis of these protocols is a must task to know its behaviour and work in that environment. Several factors will affect the overall performance of any protocol operating in an ad hoc network. For example, node mobility may cause link failures, which negatively impact on routing and quality of service (QoS) support. Network size, control overhead, and traffic intensity will have a considerable impact on network scalability along with inherent characteristics of ad hoc networks may result in unpredictable variations in the overall network performance.

Ad hoc wireless network is a unique wireless network lacking backbone infrastructure. Flexibility and quickly deployable characters of wireless ad hoc networks are due to this aspect. However, this property possesses major technological challenges. These challenges include issues of efficient routing, medium access, power management, security and quality of service (QoS). The nodes correspond over wireless links and so the nodes must be able to fight against the unpredictable character of wireless channels and interference from the additional transmitting nodes. Though the user required QoS in wireless ad hoc networks is achieved, these factors lead to a challenging problem in the direction of data throughput. Either a direct link or a multi-hop route is used for the communication between source nodes and destination nodes. For this, it is necessary that all nodes should have some fundamental routing potential to make sure that packets are delivered to their relevant destinations. While implementing ad hoc networks, huge complications occur due to the frequent route changes, which is due to the mobility of the nodes and intrusion between nodes.

2 MANET Routing Protocols

This section briefly describe the key features of the AODV, DSDV, OLSR and DSR protocols studied in our simulations. We also describe the particular parameters that we choose when implementing each protocol. But before that the basic differences in these protocol implementation lies in the mechanisms they followed according to routing strategy based classification as reactive and proactive protocols. In Reactive or on- demand routing routes are only discovered when they are actually needed. Hence, a node that wants to send a packet to another node, the reactive protocols searches for the route in an on- demand basis and establishes a connection to transmit and receive a packet.

MANET routing protocols can be categorized into 2classesas: tabledriven/proactive and source initiated (demand-driven)/reactive. This section present the overview of these protocols.

The route discovery typically consists of network wide flooding of request message. In contrast, in proactive routing each node continuously maintain route between pair of nodes. Hence, route creation and maintenance is accomplished through some combination of periodic and event - triggered routing updates derived from distance -vector or link - state method. Both these approaches have some advantages as well as some Disadvantages and can be analyzed from its performance metrics as discussed in next section.This part focused on AODV and DSR as reactive protocol and DSDV and OLSR as link- state proactive protocol.

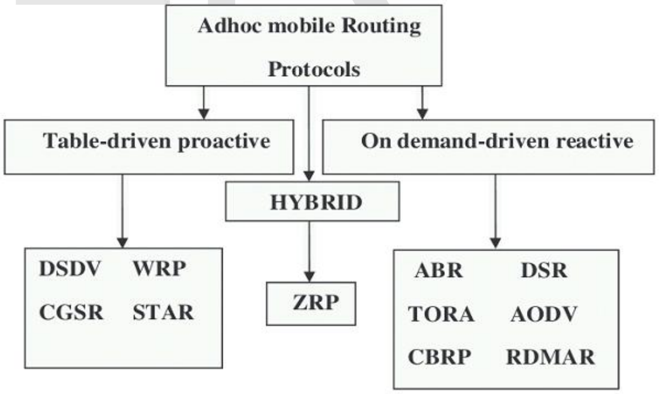


Figure :Routing protocols

2.1 Table-driven routing protocols

Table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and they respond to changes in network topology by propagating updates throughout the network in order to maintain a consistent network view. The areas in which they differ are the number of necessary routing-related tables and the methods by which changes in network structure are broadcast. The following sections discuss some of the existing table-driven ad hoc routing protocols.

2.1.1 **Destination Sequenced Distance Vector** (DSDV)

DSDV is a hop-by-hop distance vector routing protocol requiring each node to periodically broadcast routing updates based on the id ea of classical Bellman- Ford Routing algorithm [8]. Each node maintains a routing table listing the "next hop" for each reachable destination, number of hops to reach destination and the sequence number assigned by destination node. The sequence number is used to distinguish stale routes from new ones and thus avoid loop formation. The stations periodically transmit their routing tables to their immediate neighbors. A station also transmits its routing table if a significant change has occurred in its table from the last update sent. So, the update is both time - driven and event - driven. The routing table updates can be sent in two ways: a "full dump" or an "incremental" update.

2.1.2 **Optimized Link State Routing** *(OLSR)*

OLSR is an optimization of pure link state algorithm, uses the concept of Multi point Relays (MPR) for forwarding control traffic, intended for diffusion into the entire network. The MPR set is selected such that it covers all nodes that are two hops away. Due to proactive nature, OLSR works with a periodic exchange of messages like Hello messages and Topology Control (TC) message only through its MPR. The parameters used by OLSR to control the protocol overheads are Hello - interval parameter, TC-interval parameter, MPR coverage parameter and TC-redundancy parameter. So, contrary to classic link state algorithm, instead of all links, only small subsets of links are declared.

2.1.3 **Wireless routing protocol** *(WRP)*

Wireless routing protocols (WRP) is a path-finding algorithm with the exception of avoiding the count-to-infinity problem by forcing each node to perform consistency checks of predecessor information reported by all its neighbors. WRP is a loop free routing protocol. Each node maintains 4 tables: distance table, routing table, link cost table & message retransmission list table. Link changes are propagated using update messages sent between neighboring nodes. Hello messages are periodically exchanged between neighbors. This protocol avoids count-to-infinity problem by forcing each node to check predecessor information.

2.2 On demand-driven reactive protocols

On demand protocols create routes only when desired by source nodes. When a node requires a route to destination, it initiates route discovery process within the network. This process is completed once a route is found or all possible route permutations are examined.
Once a route is discovered and established, it is maintained by route maintenance procedure until either destination becomes inaccessible along every path from source or route is no longer desired.

2.2.1 Ad-hoc On -demand **Distance V***ector (AODV)*

AODV is a combination of on-demand and distance vector that is hop-to-hop routing methodology. When a node needs to know a route to a specific destination it creates a ROUTE REQUEST. Next the route request is forwarded by intermediate nodes which also create a reverse route for itself for destination. When the request reaches a node with route to destination it creates again a REPLY which contains the number of hops that are require to reach the destination. All nodes that participate in forwarding this reply to the source node create a forward route to destination. This route created from each node from source to destination is a hop-by- hop state and not the entire route as in source routing.

2.2.2 ***Dynamic Source Routing*** (***DSR***)

DSR is a simple and efficient routing protocol designed specifically for use in multihop wireless adhoc networks of mobile nodes. It allows nodes to dynamically discover a source route across multiple network hops to any destination in the adhoc network. Each data packet sent then carries in its header the complete ordered list of nodes through which the packet must pass, allowing packet routing to be a trivially loop free and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. With the inclusion of this source route in the header of each data packet, other nodes forwarding or overhearing any of the packets may easily cache this routing information for future use.

2.2.3 **Temporary-ordered routing algorithm** *(TORA)*

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive loop-free distributed routing algorithm based on the concept of link reversal. TORA is proposed to operate in a highly dynamic mobile networking environment. It is source initiated and provides multiple routes for any desired source/destination pair. The key design concept of TORA is the localization of control messages to a very small set of nodes near the occurrence of a topological change. To accomplish this, nodes need to maintain routing information about adjacent (one-hop) nodes. The protocol performs three basic functions: route creation, route maintenance, and route erasure.

3 ROUTING ATTACKS IN MANET

The malicious node(s) can attacks in MANET using different ways, such as sending fake messages several times, fake routing information, and advertising fake links to disrupt routing operations. In the following subsection, current routing attacks and its countermeasures against MANET protocols are discussed in detail.Here gave some important routing attacks.

3.1 **Flooding attack**

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

3.2 Blackhole attack

In a blackhole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

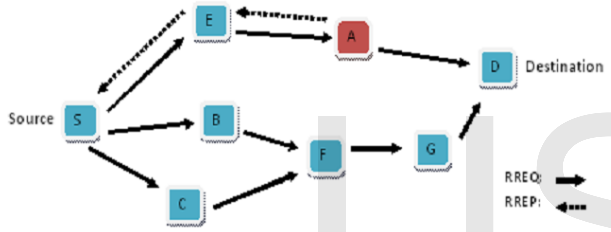


Figure 1: Blackhole attack on AODV

3.3 Link spoofing attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks. Figure 2 shows an example of the link spoofing attack in an OLSR MANET.

In the given figure, we assume that node A is the attacking node, and node T is the target to be attacked. Before the attack, both nodes A and E are MPRs for node T. During the link spoofing attack, node A advertises a fake link with node T's two-hop neighbor, that is, node D. According to the OLSR protocol, node T will select the malicious node A as its only MPR since node A is the minimum set that reaches node T's two-hop neighbors. By being node T's only MPR, node A can then drop or withhold the routing traffic generated by node T.

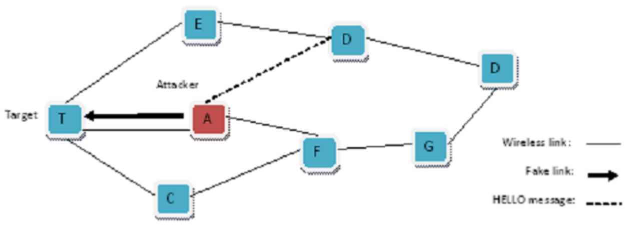


Figure 2: Link spoofing attack

3.4 Wormhole attack

A wormhole attack [13] is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Figure 3 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked.

During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbors C and E forward the RREQ as usual.

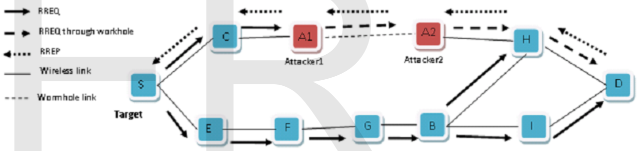
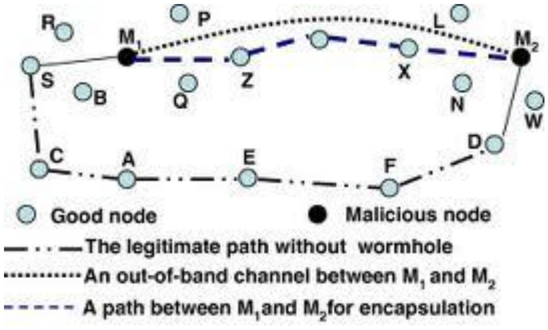


Figure 3: Wormhole attack on reactive routing

3.5 Colluding misrelay attack

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog and pathrater 16. Figure 4 shows an example of this attack. Consider the case where node A1 forwards routing packets for node T.


R
P
L
M1
M2
S
B
Q
Z
X
N
W
C
A
E
F
D
Good node
Malicious node
The legitimate path without wormhole
An out-of-band channel between M1 and M2
A path between M1 and M2 for encapsulation

In the figure, the first attacker A1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets.

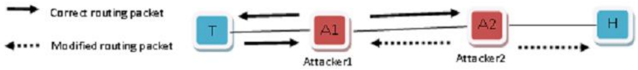


Figure 4: Colluding misrealy attack

4 Failures in Routing

Maximizing the data packet delivery in the face of fast changing network topology devoid of incurring a large routing overhead is the major issue in mobile ad hoc networks. The packet delivery ratio can be reduced by slow detection of broken links which causes the data packets to be forwarded to stale or invalid paths. The main reason for packet loss in ad hoc networks is the link failure or node failure which is due to energy draining in nodes. A link failure is caused if there is more than one packet using this link after the physical layer failure. Though after a failure, the routing protocol takes off such packets from the queue, new packets still keep coming into the queue without any checking. If the new incoming packets make use of the failed link, then they will block all other packets resulting in network wide low throughput and long delay.

Detection of link failures in an ad hoc network becomes challenging due to the lack of centralized monitoring and management point. This makes the faulty nodes to remain long time in the network, which affects the performance of routing in the ad hoc network. For instance, if a defective node participating in the routing process drops data packets, subsequently a large number of packets will be lost. In order to increase the reliability, it is needed to distinguish and moderate the failures. By knowing individual link stability along a path by calculating the node remaining energy, path stability can be identified. This can be done by means of estimating the node remaining energy.

Also securing the ad hoc networks plays an important role. For security there are algorithms which is consuming high overhead of packets and much computing time. Hence, a security mechanism is needed which consumes less overhead and reduced computation time. This paper provides an adaptive security algorithm called as Intercept detection and correction (IDC) which identifies the malicious data forwarding through the network from source, intermediate and destination nodes.

5 Trust in MANET

Trust is a critical factor which depends on uncertain conditions and is used for decision making on cooperating with unknown participants. It includes establishment and updation of trust. In general, trust management and reputation management are invariably used but it is not the fact. There lies a difference between the trust and reputation. Trust is active while reputation is passive [18]. Direct observation and recommendation are the ways used to measure trust or reputation. Recommendation is simply an effort to pass one node's trust or reputation to another.

Golbeck [21] elaborates about three main properties of trust with reference to social network. Trust cannot be completely transitive in mathematical terms. That is, if A trusts B, and B trusts C, it does not guarantee that A trusts C. Second, trust is not necessarily symmetric, meaning not identical in both directions.

Yonfang [22] Discusses about policy - based trust management and reputation based trust management. Policy based techniques uses logical rules and verifiable properties encoded in signed credential s for user access to resources. Policy based technique takes binary decision based on which the requester is trusted or not and accordingly access is decided. Due to its binary decision methodology provides less flexibility. On the other side reputation based scheme derives trust based on numerical and computational mechanism.

Trust is an inevitable property in the design and analysis of distribution systems [23]. Trust is a critical part through which the relationships emerge [24]. Proper security measure s and correct decisions shall be arrived by clarifying the trust relationship. A trust model involves specification and setting up of trust relationship among entities. Trust modeling is seen as growing technique to represent trust in digital format. Recently it has gained significance in providing security in electronic systems. Current trust academic work covers such aspects as analyzing the problems of current secure systems [25,26], proposing models for achieving trust in digital systems [27,28] and quantifying or specifying trust in digital systems. The above section depicts some of the existing trust management schemes developed for MANET environments.

6 Routing Mechanism-Module Description

6.1 LOGIN

The USER enter into login, if the user doesn't register it will move to new user creation from. In this Module Collecting the general user details and store database for future references. It having first Name, last name, username Password.

6.2 DATA TRANSFER

A data which is to be send is transferred from the source to the destination. The overall security of routed messages is thus dependent on the routing protocol implemented in the wireless network, as well as the physical network topology and the relative positions of the source and destination nodes in the network. Moreover, the fact that a message is transmitted over numerous links between a source and destination node implies that the overall confidentiality and integrity of the routed message may only be as secure as the least secure link, implying that vulnerabilities arise due to the topology of secure links in the wireless network.

6.3 PRE AUTHENTICATION METHOD

To reduce the message processing delay, authentication is done during scanning phase. By the method, the authentication delay vanishes and the message processing delay (α), is composed only of the re-association time. Thus the parameter 'α' is reduced by at least half of its initial value and hence the net time delay, t, as proposed, is greatly reduced. It can be implemented as proposed in performance analysis . Thus, the authentication time, which was very minute in proportion as compared to scanning phase delay of previous methods, would now command a greater percent of time delay, because, in our case, the scanning phase delay has been much reduced.

6.4 IDENTIFYING THE VULNERABILITY

In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated. The notion of risk can be adopted to support more adaptive responses to routing attacks in MANET Another unique characteristic of MANET is the dynamic nature of its network topology which would be frequently changed due to the unpredictable mobility of nodes. Each mobile node in MANET plays a router role while transmitting data over the network. Hence, any compromised nodes under an adversary's control could cause significant damage to the functionality and security of its network since the impact would propagate in performing routing tasks.

6.5 EVALUATION OF VULNERABILITY

The vulnerability in transferring a data from the sender to the receiver is evaluated in this module. Messages in a wireless network traverse multiple links and paths between a source and destination node, and a message may be compromised by traversing a single insecure link. Nowadays networks are growing in a haphazard manner and use data, money transaction, information etc. Even though internet plays a vital role it is subject to some vulnerability.

6.6 AVOID THE VULNERABILITY

The vulnerability is avoided in the data transmission providing a secure data transfer without the attack by the use of route path efficiently. A practical IP trace back system called Flexible Deterministic Packet Marking which provides a defense system for IP packets and denial service attacks that traverse through the network has been elucidated in this study. The vulnerability is avoided in the data transmission providing a secure data transfer without the attack by the use of route path efficiently.

6.7 PERFORMANCE ANALYSIS

To evaluate the effectiveness of our adaptive risk-aware response solution, we divided the simulation process into three stages and compared the network performance in terms of six metrics. The following describes the activities associated with each stage Stage 1-Before attack. Random packets were generated and transmitted among nodes without activating any of them as attackers. This simulation can present the traffic patterns under the normal circumstance. Stage 2-After attack. Specific nodes were set as attackers which conducted malicious activities for their own profits. However, any detection or response is not available in this stage. The security provides a good routing path in delivering the data to the destination avoiding the attacks.

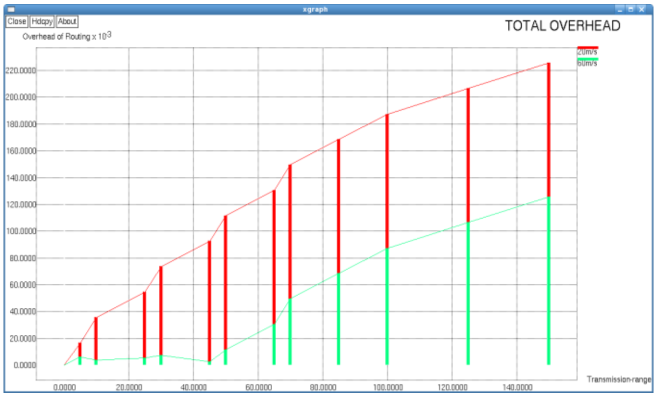


Fig. 5: Total ***Overhead***

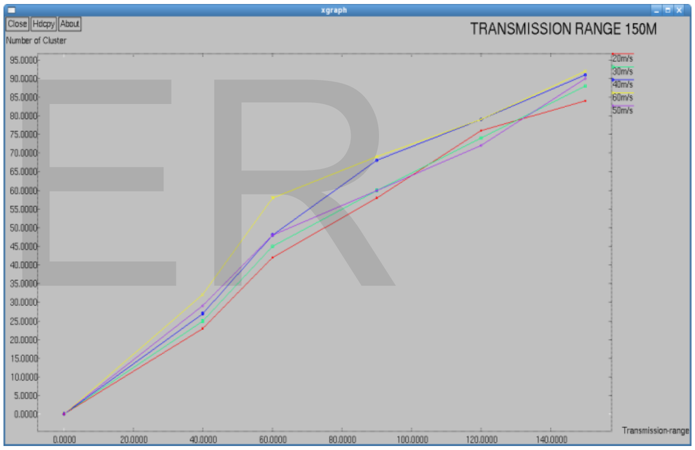


Fig. 6: Transmission range

7 EXISTING DEMPSTER-SHAFER THEORY OF EVIDENCE

The Dempster-Shafer mathematical theory of evidence is both a theory of evidence and a theory of probable reasoning. The degree of belief models the evidence, while Dempster's rule of combination is the procedure to aggregate and summarize a corpus of evidences.

However, previous research efforts identify several limitations of the Dempster's rule of combination Dempster-Shafer theory offers an alternative to traditional probabilistic theory for the mathematical representation of uncertainty. The significant innovation of this framework is that it allows for the allocation of a probability mass to sets or intervals. Dempster-Shafer theory does not require an assumption regarding the probability of the individual constituents of the set or interval.

7.1 DISADVANTAGES OF DS THEORY:

The research reviewed in this survey has also shown that the use of D-S theory has certain disadvantages. They are mentioned below.

Disadvantages of Dempster-Shafer evidence theory for active fusion and compare evidence theory with Dayesian and fuzzy modeling.

According to Siaterlis et al. [2003], Siaterlis and Maglaris [2004 and 2005], and Chatzigiannakis et al. [2007] the main disadvantage of the D-S theory is that the assumption it makes that the pieces of evidence is statistically independent from each other. Since sources of information are often linked with some sort of dependence in real life situations, this assumption does not always hold true. Also, in the Siaterlis et al. [2003] framework, they pointed out that the systems inability to detect multiple simultaneous attacks. This was because they assumed a mutually exclusive set of system states.

According to Chen and Aickelin [2006], D-S has two major problems. One they say is the computational complexity associated with D-S. The other is the conflicting beliefs management. According to Chen and Aickelin the computational complexity of D-S increases exponentially with the number of elements in the frame of discernment (Θ). If there are n elements in Θ, there will be up to 2^n-1 focal elements for the mass function. Further the combination of two mass functions needs the computation of up to 2^n intersections.

Yager [10] and Yamada and Kudo [18] proposed rules to combine several evidences presented sequentially for the first limitation. Wu et al. [11] suggested a weighted combination rule to handle the second limitation. However,the weight for different evidences in their proposed rule is ineffective and insufficient to differentiate and prioritize different evidences in terms of security and criticality. Our extended Dempster-Shafer theory with importance factors can overcome both of the aforementioned limitations.

8 RISK –AWARE RESPONSE MECHANISM

In this section, we articulate an adaptive risk-aware response mechanism based on quantitative risk estimation and risk tolerance. Instead of applying simple binary isolation of malicious nodes, our approach adopts an isolation mechanism in a temporal manner based on the risk value. We perform risk assessment with the extended D-S evidence theory introduced for both attacks and corresponding countermeasures to make more accurate response decisions illustrated in Fig. 1.

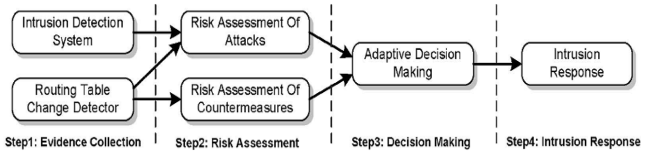

Intrusion Detection System
Routing Table Change Detector
Risk Assessment Of Attacks
Risk Assessment Of Countermeasures
Adaptive Decision Making
Intrusion Response
Step1: Evidence Collection
Step2: Risk Assessment
Step3: Decision Making
Step4: Intrusion Response

Fig.7: Risk-aware response mechanism.

8.1 OVERVIEW

Because of the infrastructure-less architecture of MANET, our risk-awa re response system is distributed, which means each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET may isolate the malicious node, but others may still keep in cooperation with due to high dependency relationships. Our risk-aware response mechanism is divided into the following four steps shown in Fig.1

Evidence collection: In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value, and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.

Risk assessment: Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and the risk of countermeasures, the entire risk of an attack could be figured out.

Decision making: The adaptive decision module provides a flexible response decision-making mechanism, which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfill her goal.

Intrusion response: With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner.

8.2 Response to Routing Attacks

In this approach, we use two different responses to deal with different attack methods: routing table recovery and node isolation. Routing table recovery includes local routing table recovery and global routing recovery. Local routing recovery is performed by victim nodes that detect the attack and automatically recover its own routing table.

Global routing recovery involves with sending recovered routing messages by victim nodes and updating their routing table based on corrected routing information in real time by other nodes in MANET.

Routing table recovery is an indispensable response and should serve as the first response method after successful detection of attacks. In proactive routing protocols like OLSR, routing table recovery does not bring any additional overhead since it periodically goes with routing control messages. Also, as long as the detection of attack is positive, this response causes no negative impacts on existing routing operations.

Node isolation may be the most intuitive way to prevent further attacks from being launched by malicious nodes in MANET. To perform a node isolation response, the neighbors of the malicious node ignore the malicious node by neither forwarding packets through it nor accepting any packets from it. On the other hand, a binary node isolation response may result in negative impacts to the routing operations, even bringing more routing damages than the attack itself.

In Fig. 2, Node 1 behaves like a malicious node. However, if every other node simply isolate Node 1, Node 6 will be disconnected from the network. Therefore, more flexible and fine-grained node isolation mechanism are required. In our risk-aware response mechanism, we adopt two types of time-wise isolation responses: temporary isolation And permanent isolation.

9 PROPOSED GNAVE ALGORITHM (GREEDY NODE CAPTURE APPROXIMATION USING VULNERABILITY EVALUATION)

We define a class of route vulnerability metrics (RVMs) to quantify the effective security of traffic traversing a given route. Using the RVM definition, we formulate the minimum cost node capture attack problem as a nonlinear integer programming minimization problem. Since determining the optimal node capture attack is likely infeasible, propose the GNAVE algorithm using a greedy heuristic to iteratively capture nodes which maximize the increase in route vulnerability.

Advantage:

- It is applicable for single and multipath routing.
- Our proposed metric captures the gain achieved due to information leakage by the joint consideration of the routing and key assignment protocols.
- There is no computational complexity in this algorithim.
- It's very efficeint and cheap and providing more security.
- Survival of vulnerability attacks in the network.
- Secure transfer of data.
- Provides confidentiality, integrity of data.
- Provides reliable data transfer.
- Survival of vulnerability attacks in the network.

10 LITERATURE REVIEW

To investigate the impact of node capture attacks on the confidentiality and integrity of network traffic. We map the compromise of network traffic to the flow of current through an electric circuit and propose a metric for quantifying the vulnerability of the traffic using the circuit mapping. We compute the vulnerability metric as a function of the routing and the cryptographic protocssols used to secure the network traffic. We formulate the minimum cost node capture attack problem as a nonlinear integer programming problem. Due to the NP-hardness of the minimization problem, we provide a greedy heuristic that approximates the minimum cost attack. We provide examples of node capture attacks using our vulnerability metric and show that the adversary can expand significantly less resources to compromise target traffic by exploiting information leakage from the routing and cryptographic protocols.

Recent work on network coding renders a new view on multicasting in a network. In the paradigm of network coding, the nodes in a netwossrk are allowed to encode the information received from the input links. The usual function of switching at a node is a special case of network coding. The advantage of network coding is that the full capacity of the network can be utilized. In this paper, we propose a new model which incorporates network coding and information security. Specifically, a collection of subsets of links is given, and a wire tapper is allowed to access any one (but not more than one) of these subsets without being able to obtain any information about the message transmitted. Our model includes secret sharing as a special case. We present a construction of secure linear network codes provided a certain graph-theoretic sufficient condition is satisfied.

11 IMPLEMENTATION

Implementation is the process of converting the logical system design into the physical system design. The implementation plan involves physical system design, physical database system, program development data collection and change over. This is the final stage of system development and more attention is imperative.
The various programming languages are analyzed for their capability to provide such a system. Client server technology was selected for creating the system. Among the software, which supports client server technology, C#.Net and MS-SQL Server are considered for its easy programming and faster execution.

The goal of the program development phase is developing code. For each module of the system, sub procedures are written for retrieving, processing, updating, storing data into the tables. Sub procedures are a set of C# commands used to do a particular task. Reports are generated using Crystal Reports.

The studies on node capture attacks have all focused on the ability of an adversary to compromise the security of single-hop wireless links. However, messages in a wireless network traverse multiple links and paths between a source and destination node, and a message may be compromised by traversing a single insecure link. The overall security of routed messages is thus dependent on the routing protocol implemented in the wireless network, as well as the physical network topology and the relative positions of the source and destination nodes in the network.

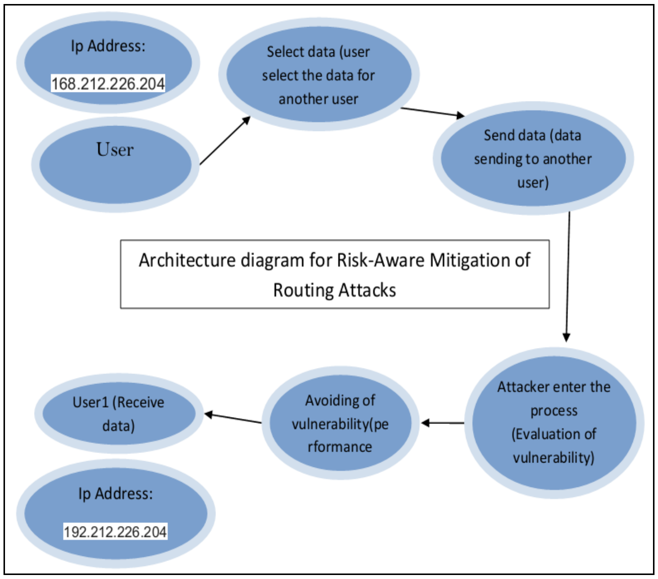

Ip Address:
168.212.226.204
User
Select data (user select the data for another user
Send data (data sending to another user)
Architecture diagram for Risk-Aware Mitigation of Routing Attacks
Attacker enter the process (Evaluation of vulnerability)
Avoiding of vulnerability(performance
User1 (Receive data)
Ip Address:
192.212.226.204

Fig 8: Architecture diagram for mitigation of rouring attacks

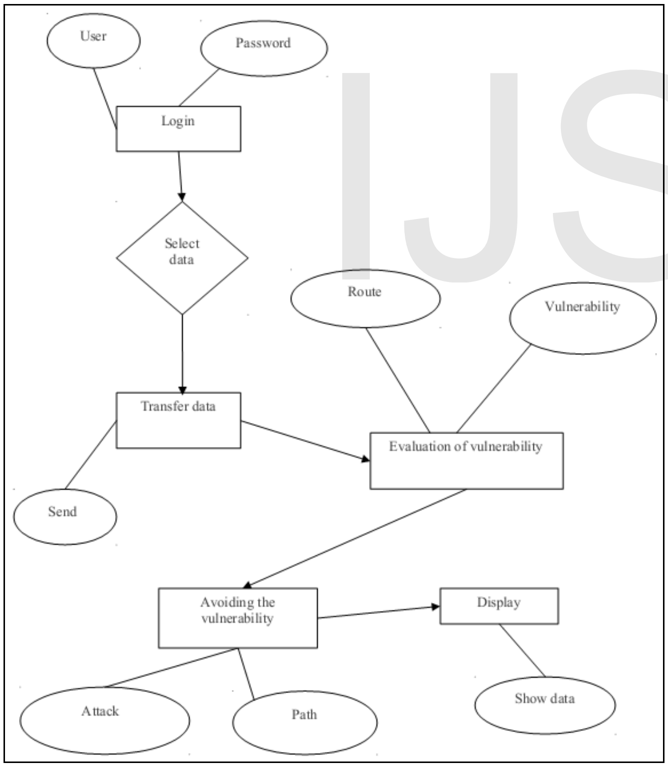


Fig 9: Overall architecture

Moreover the fact that a message is transmitted over numerous links. This links between a source and destination node implies that the overall confidentiality and integrity of the routed message may only be as secure as the least secure link, implying that vulnerabilities arise due to the topology of secure links in the wireless network. Hence, the impact of a node capture attack is a function of both the cryptographic protocol which provides link security and the routing protocol which determines the set of links traversed by a given message.

FUTURE PLAN

This application has been developed to overcome the problems in the present manual systems. It is flexible to use in buy the products and pet store and other details of the management. For further improvement, the back-end tool can be modified or changed to the SQL server. So it would enhance the instructiveness of the software with additional features for the Windows XP Operating System. Hardware configuration changes also should increase the speed of software utility. The databases also designed such that to make modification or further improvement in the production department of the mill. It may be included in the database.

11. Conclusion

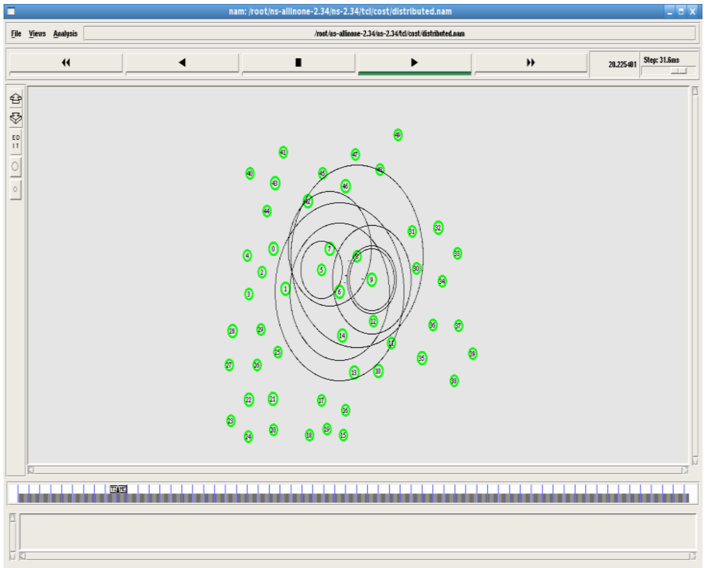
This chapter examined the main security issues in MANETs. They have most of the problems of wired networks and many more besides due to their specific features: dynamic topology, limited resources (*e.g.* bandwidth, power), lack of central management points. Firstly we have presented specific vulnerabilities of this new environment. Then we have surveyed the attacks exploit these vulnerabilities and, possible proactive and reactive solutions proposed in the literature.

Attacks are classified into passive and active attacks at the top level. Since proposed routing protocols on MANETs are insecure, we have mainly focused on active routing attacks which are classified into dropping, modification, fabrication, and timing attacks. Attackers have also been discussed and examined under insider and outsider attackers. Insiders attacks are also examined.

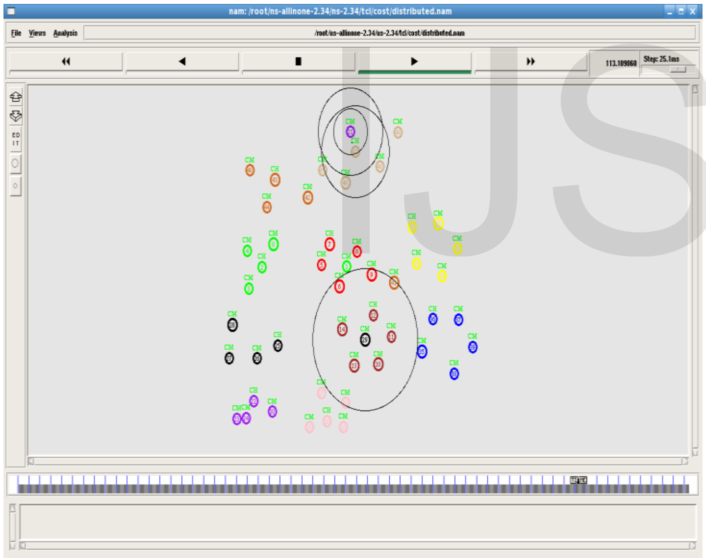
Conventional security techniques are not directly applicable to MANETs due to their very nature. Researchers currently focus on developing new prevention, detection and response mechanism for MANETs. In this chapter we summarize secure routing approaches proposed for MANETs. The difficulty of key management on this distributed and cooperative environment is also discussed. Furthermore we have surveyed intrusion detection systems with different detection techniques proposed in the literature. Each approach and technique is presented with attacks they can and cannot detect. To conclude, MANET security is a complex and challenging topic. To propose security solutions well-suited to this new environment, we recommend researchers investigate a possible security risks to MANETs most thoroughly.

Acknowledgments

I would pay My sincere devotion to the Almighty and My Parents, who filled me with wisdom and knowledge and rendered me good health and made me to finish this project successfully. The satisfaction and delight that accompany the successful completion of any task would be incomplete without mentioning the people who were responsible for the completion of the project. Last but not the least I thank to all my friends for their moral support and technical discussions in doing the project.


nam: /root/ns-allinone-2.34/ns-2.34/tcl/cost/distributed.nam
File
Views
Analysis
/root/ns-allinone-2.34/ns-2.34/tcl/cost/distributed.nam
20.225401
Step: 31.6ms

Screen shot 1: Node communication


nam: /root/ns-allinone-2.34/ns-2.34/tcl/cost/distributed.nam
File
Views
Analysis
/root/ns-allinone-2.34/ns-2.34/tcl/cost/distributed.nam
113.109060
Step: 25.1ms

Screen shot 2: Attack detection

REFERENCES

[1] Y. Sun, W. Yu, Z. Han, and K. Liu, “Information TheoreticFramework of Trust Modeling and Evaluation for Ad Hoc Networks,”IEEE J. Selected Areas in Comm., vol. 24, no. 2, pp. 305-317, Feb. 2006.

[2] M. Refaei, L. DaSilva, M. Eltoweissy, and T. Nadeem, “Adaptation of Reputation Management Systems to Dynamic Network Condi-tions in Ad Hoc Networks,” IEEE Trans. Computers, vol. 59, no. 5, pp. 707-719, May 2010.

[3] P. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner, and A. Reninger, “Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control,”Proc. 28th IEEE Symp. Security and Privacy, 2007.

[4] S. Wang, C. Tseng, K. Levitt, and M. Bishop, “Cost-Sensitive Intrusion Responses for Mobile Ad Hoc Networks,” Proc. 10th Int’l Symp. Recent Advances in Intrusion Detection (RAID ’07), pp. 127-145, 2007.

[5] G. Shafer,A Mathematical Theory of Evidence. Princeton Univ., 1976.

[6] L. Sun, R. Srivastava, and T. Mock, “An Information Systems Security Risk Assessment Model under the Dempster-Shafer Theory of Belief Functions,”J. Management Information Systems, Vol. 22, no. 4, pp. 109-142, 2006.

[7] C. Mu, X. Li, H. Huang, and S. Tian, “Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory,” Proc. 13th European Symp. Research in Computer Security (ESORICS ’08), pp. 35-48, 2008.

[8] K. Sentz and S. Ferson, “Combination of Evidence in Dempster-Shafer Theory,” technical report, Sandia Nat’l Laboratories, 2002.

[9] L. Zadeh, “Review of a Mathematical Theory of Evidence,” AI Magazine,vol. 5, no. 3, p. 81, 1984.

[10] R. Yager, “On the Dempster-Shafer Framework and New Combination Rules 1,” Information Sciences, vol. 41, no. 2, pp. 93-137, 1987.

[11] H. Wu, M. Siegel, R. Stiefelhagen, and J. Yang, “Sensor Fusion Using Dempster-Shafer Theosry,” Proc. IEEE Instrumentation and Measurement Technology Conf.,vol. 1, pp. 7-12, 2002.

[12] T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol,” Network Working Group, 2003.

[13] C. Perkins, E. Belding-Royer, and S. Das, “Ad Hoc On-Demand Distance Vector Routing,” Mobile Ad-Hoc Network Working Group, vol. 3561, 2003.

[14] H. Deng, W. Li, and D. Agrawal, “Routing Security in Wireless Ad Hoc Networks,” IEEE Comm. Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

[15] Y. Hu and A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing,”IEEE Security and Privacy Magazine, vol. 2, no. 3, pp. 28-39, May/June 2004.

[16] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “A Survey of Routing Attacks in Mobile Ad Hoc Networks,”IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[17] C. Karlof and D. Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Ad Hoc Networks, vol. 1, nos. 2/3, pp. 293-315, 2003.

[18] M. Yamada and M. Kudo, “Combination of Weak Evidences by D-S Theory for Person Recognition,”Knowledge-Based Intelligent Information and Engineering Systems, pp. 1065-1071, Springer, 2004.

[19] K. Fall and K. Varadhan, “The NS Manual,” 2010.

[20] F. Ros, “UM-OLSR Implementation (version 0.8.8) for NS2,” 2007.

Author's Biographies

Jaganraj *A* received the BE degree from Arunai Engineering College Which affiliated to Anna University, Chennai, India, in 2010. He is currently pursuing the Master Degree in Arulmigu Meenakshi Amman college of engineering which is Affiliated to Anna University, Chennai. His research interests include malicious node analysis, web and internet security, and wireless network security.
E-mail: jagan_math88@yahoo.co.in.

Aishwarya K received the ME degree from Anna University Chennai in 2011 and joined as an Assistant Professor in various engineering colleges in Tamil Nadu affiliated to Anna University and has four year teaching experience. She has a membership in computer society of India. She has published papers in international journals. Her current primary area of research is Network Security and Wireless communication.
E-mail: aishumecse@gmail.com

Yogaraj A received the BE degree from Kamban Engineering College Which affiliated to Anna University, Chennai, India, in 2006. Also He received M.Tech degree From Anna University, Chennai, India, in 2009. He is currently working as Assistant Professor in Veltech Dr.R.R & Dr.S.R Technical University, Avadi, Chennai since 2009. His research interests include neural network, Optical Fiber Communication, Nano science & technology and communication system.
E-mail: yoga.rajam@yahoo.co.in