ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Secure Routing Protocol in Delay Tolerant Networks Using Fuzzy Logic Algorithm

S.Karthika, N.Vanitha

M.E Student [Applied Electronics], Dept. of ECE, Kingston Engineering College, Vellore, Tamil Nadu, India

Assistant Professor, Dept. of ECE, Kingston Engineering College, Vellore, Tamil Nadu, India

ABSTRACT: Security is the biggest challenge in MANET. MANET presents various types of security attacks on data exchanges taking place between source and destination. In this misbehavior detection schemes for conventional wireless networks has opposed black hole attack and malicious node occur routing, this proposed technique as a great challenges in networks. In this iTrust, a probabilistic misbehavior detection scheme is highly desirable to assure the secure DTN routing as well as the establishment of the trust, among DTN nodes. A zone (routing zone) of a node is used to collect the node information within the range. In this protocol, it cannot achieve the packet delivery ratio, performance and data loss rate. In this paper we are providing the solution against black hole attack which is based on fuzzy rule. Fuzzy rule is used to identify the infected node as well as provide the solution to reduce data loss over network. Fuzzy logic ranges between the value as {0, 1}. Geographic routing is one of the most suitable routing strategies in wireless mobile Adhoc network mainly due to its scalability. Multi Input Multi Output technique used to send data frequently in routing protocol. Analysis and simulation results demonstrate the effectiveness and efficiency of the drop node analysis, high packet delivery ratio, throughput and delay.

KEYWORDS*:* Security; DTN; Malicious Node; I trust; Fuzzy logic; MIMO, Geographic routing.

I. INTRODUCTION

A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure. This type of network, operating as a stand-alone network or with one or multiple points of attachment to cellular networks or the Internet, paves the way for new and exciting applications. Application scenarios include, but are not limited to emergency and rescue operations, conference or campus settings, car networks, personal networking, etc.

A mobile ad hoc network (MANETs) is an infrastructure-less, dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. Due to its fundamental characteristics, such as wireless medium, dynamic topology, distributed cooperation, MANETs is vulnerable to various kinds of security attacks like worm hole, black hole, rushing attack etc.

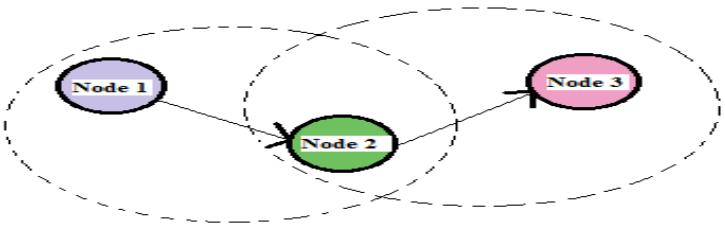

Fig 1: Mobile Adhoc Networks

Securing wireless ad-hoc networks is a highly challenging issue. Understanding possible form of attacks is always the first step towards developing good security solutions. Security of communication in MANET is important

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

for secure transmission of information. Absence of any central co-ordination mechanism and shared wireless medium makes MANET more vulnerable to digital/cyber attacks than wired network there are a number of attacks that affect MANET.

II. RELATED WORK

A.*ZONE ROUTING PROTOCOL:*

The proposed protocol is based on the concept zone routing protocol (ZRP). It employs an integrated approach of digital signature and both the symmetric and asymmetric key encryption techniques to achieve the security goals like message integrity, data confidentiality and end to end authentication at IP layer. The thesis details the design of the proposed protocol and analyses its robustness in the presence of multiple possible security attacks that involves impersonation, modification, fabrication and replay of packets caused either by an external advisory or an internal compromised node within the network. The Zone Routing Protocol (ZRP) as described in aims at addressing these limitations by combining the best properties of both proactive and reactive approaches and hence it can be classed as a hybrid proactive/reactive routing protocol. A zone (routing zone) of a node is nothing but local neighbourhood of that node.

B. *RSA (Rivets Shamir Adelman) Algorithm:*

Black hole attack arises in route discovery phase. Essentially black hole attack is change of hop and immediate response using sequence number in the field of RREQ (Route Request). It involves three steps: Key Generation, Encryption and Decryption. The Encryption method the destination node sends the message public key to source node. The private key keeps the information secret then source node send the message to destination node. The decryption method the destination node recovers the original message. The original message can be received using decrypt method.

C. *Trusted Authority:*

The trade-off between the security and detection cost, iTrust introduces a periodically available Trust Authority which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Then TA could punish or compensate the node based on its behaviors. to further improve the performance of the proposed probabilistic inspection scheme. we introduce a reputation system, in which the inspection probability could vary along with the target node's reputation. Under the reputation system, a node with a good reputation will be checked with a lower probability while a bad reputation node could be checked with a higher probability. We model iTrust as the Inspection Game and use game theoretical analysis to demonstrate that TA could ensure the security of dtn routing at a reduced cost via choosing an appropriate investigation probability. . So if we don't consider network constraints, F should fully match Delegation Task D. However, in reality, node B may fail to finish all of the tasks due to the network constraints (e.g., lack of enough contacts).

III. PROPOSED METHODOLOGY

A. *Delay Tolerant Networks:*

A DTN is a network of smaller networks. It is an overlay on top of special-purpose networks, including the Internet. DTNs support interoperability of other networks by accommodating long disruptions and delays between and within those networks, and by translating between the communication protocols of those networks. In providing these functions, DTNs accommodate the mobility and limited power of evolving wireless communication devices. DTNs were originally developed for interplanetary use, where the speed of light can seem slow and delay-tolerance is the greatest need.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

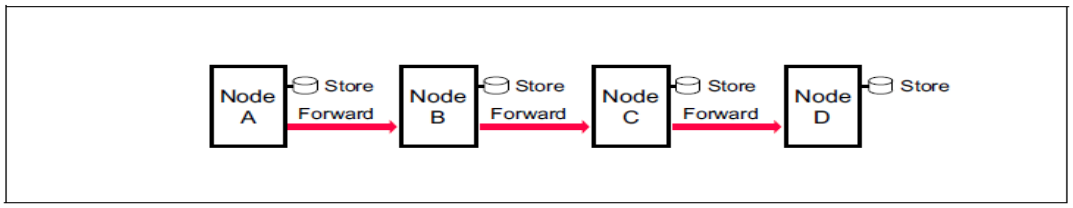

Fig 2: Store and Forward Methods

Store-and-forwarding methods are also used in today's voicemail and email systems, but these systems are not node-to-node relays (as shown above) but rather star relays; both the source and destination independently contact a central storage device at the centre of the links. The storage places (such as hard disk) can hold messages indefinitely. They are called persistent storage, as opposed to very short-term storage provided by memory chips and buffers. Internet routers use memory chips and buffers to store (queue) incoming packets for a few milliseconds while they are waiting for their next-hop routing-table lookup and an available outgoing router port.

B. Black Hole Attack:

Malicious node in the network is called as black hole as shown in Figure 3. Black hole intercepts the packet and the confidentiality of the message is disclosed. In black hole attack, the malicious node waits for neighbouring nodes to send RREQ messages. When the malicious node receives RREQ, it immediately sends RREP with highest sequence number to the source before any other node sends RREP. Source node on receiving RREP with high sequence number, establishes route to black hole node and start transmitting packets assuming that the node knows the route to the sink node. Malicious node attack all RREQ messages this way and takes over all routes. In such attacks, all packets in the network are being sent to a point from where they are not forwarding to anywhere. This is called black hole, meaning which swallows all objects and matter.

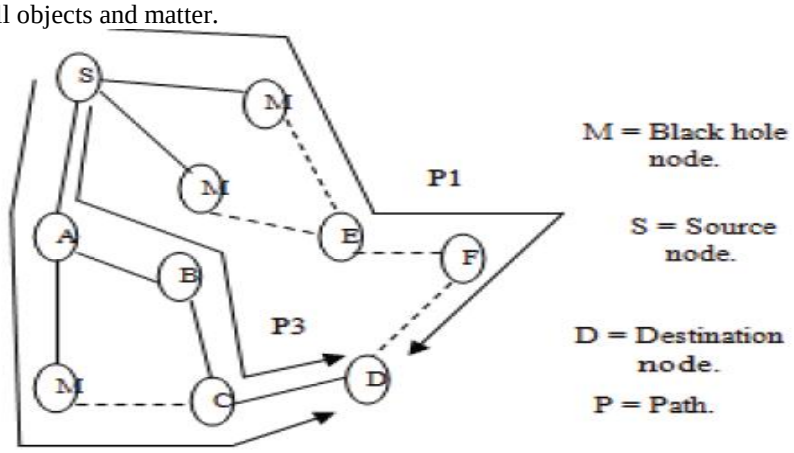

Fig 3: Example of Black-hole attack

C. Fuzzy Logic Algorithm:

The proposed system is about to design an intrusion detection system to detect the black hole attack on MANET This detection system is based on FUZZY LOGIC. We propose an IDS system in which improvement is by making use of two factors i.e. Packet Loss rate, Data Rate. We will use both factors using Fuzzy logic which is problem solving control system .Fuzzy logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, noisy or missing information. We proposed an algorithm which is based on above factors. In this algorithm firstly we define the network with N number of nodes and we set source node to S and destination node D and after that we let current node is as source node .we repeat the steps until current node is not equal to destination node.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

D. *Algorithm to Detect the Black Hole Attack:*

1. Define a Network with N number of nodes
2. Define the Source Node S and Destination Node D
3. Set Cur Node=S as Current Node
4. While Cur Node <> DestNode a. [Repeat Steps 5 to 40]
5. Identify the list of neighboring nodes to Cur Node called Ne(1),Ne(2)…..Ne(M)
6. For i=1 to M
7. {
8. Identify the Analysis parameter for Each Neighbor called Packet Loss rate, Data Rate
9. [Sender End Fuzzy Logic]
10. Fuzzily these rules under the fuzzification process
11. If (Fuzzy (Packet Loss rate (Ne (i)), Low) and Fuzzy (Data Rate (Ne (i)), High)
12. {
13. Set Priority (Ne (i)) =High
14.}
15. Else If (Fuzzy(Packet Loss rate(Ne(i)),Medium)and Fuzzy(Data Rate(Ne(i)),Medium)
16. {
17. Set Priority (Ne (i)) =Medium
18.}
19. Else If (Fuzzy (Packet Loss rate (Ne (i)), Low) and Fuzzy (Data Rate (Ne (i)), Low)
20. {
21. Set Priority (Ne (i)) =Low. (Black hole node found)
22.}
23.}
24. Find the List of High Priority Receivers from the Neighbor List called P (1), P (2)….P (K)
25. [Receiver level Fuzzy Logic]
26. For i=1 to K
27. {
28. If (Energy (P (i)) =Low)
29. {
30. Set Priority (P (i)) =Low
31.}
32. If(Data Transmitted(P(i))>THRESHOLD and Rate(P(i))>THRESHOLD)
33. {
34. Set Priority (P (i)) =priority (P (i)) +1
35.}
36.}
37.}
38. Find the Node with Max Priority called Node p
39. Set Cur Node=p
40.}

E**.** *Geographic Routing:*

"Geographic routing" is mainly a solution that employs geographic information for the purpose of routing and data forwarding. Thus, the focus in this report is mainly on such protocols and when we use the term "geographic routing", we refer to this category of routing protocols. Geographic routing protocols scale better for ad hoc networks mainly for two reasons: There is no necessity to keep routing tables up-to-date and No need to have a global view of the network topology and its changes. Therefore, geographic routing protocols have attracted a lot of attention in the field of routing protocols for MANETs. These geographic approaches allow routers to be nearly stateless because forwarding decisions are based on location information of the destination and the location information of all one-hop neighbours. Most of these protocols keep state only about the local topology (i.e., neighbours' location information).

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

F. *Multi Input Multi Output (MIMO):*

High data rate wireless communications links with transmission rates nearing 1 Gigabit/second (will quantify a "bit" shortly)Provide high speed links that still offer good Quality of Service (QoS) (will be quantified mathematically).We focus on the MIMO (Multi-Input and Multi-Output) technology to overcome these drawbacks and to significantly improve the monitoring process. We propose a new MAC protocol called MIMO .MAC based on the well-known SPACE-MAC protocol. It allows the monitor node to avoid the collision during the monitoring process by adjusting the antennas weights in order to nullify the signal coming from other nodes than the monitored one. Therefore, the proposed solution contributes to significantly enhance the accuracy of the monitoring process. The main advantage of SPACE-PAC is that it allows multiple data streams at the same time in the same collision area, thereby increasing the overall capacity of the network**.**

IV. EXPERIMENTAL RESULTS

NS2.35 Network simulator is used to simulate a wireless network with DTN protocol. These nodes are labelled; ranging from Node 0 to Node 24. Constant Bit Rate (CBR) traffic is set. The simulation detects the malicious nodes based on computed trust values. We calculate the parameters like packet delivery ratio, packet drop analysis, throughput, data loss rate and end to end delay are calculated by using the trace file.

Parameters	Values
Simulator	NS2.35
Routing protocol	DTN
Number of nodes	25
Frequency	10^{-3} Hz
Simulation time	600ms
Algorithm	Fuzzy

Table 1: Simulation Parameter

A.PACKET DELIVERY RATIO:

In our parameter, while the packet delivery ratio is decrease in black hole DTN when compare to the ZRP. In our system there was 0.5% of malicious node occur in the black hole. PDR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source. In this graph for 25 nodes, existing model detects less number of malicious nodes. In the proposed work, detection of malicious node is higher than that of the existing models.

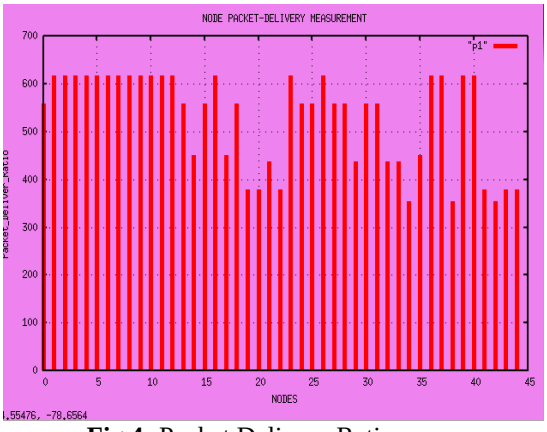

Fig 4: Packet Delivery Ratio

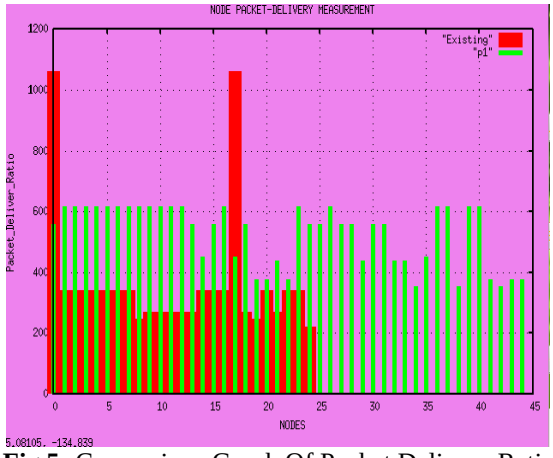

Fig 5: Comparison Graph Of Packet Delivery Ratio

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

B. *Data Packet Loss Rate:*

In this paper , we discuss about the fuzzy algorithm to detect the malicious nodes. Fuzzy ranges between the values of {0,1}.Fuzzy algorithm used the value of '0' represent to detect the malicious nodes and '1' represent the normal nodes. Fuzzy rule based solution identify the infected node as well as provide the solution to reduce data loss over network**.** In our parameter, while the data packet loss rate is decrease in black hole DTN when compare to the ZRP. In our system there was 0.5% of malicious node occur in the black hole. PLR is the ratio of the number of data packets received by the destination to the number of data packets sent by the source.

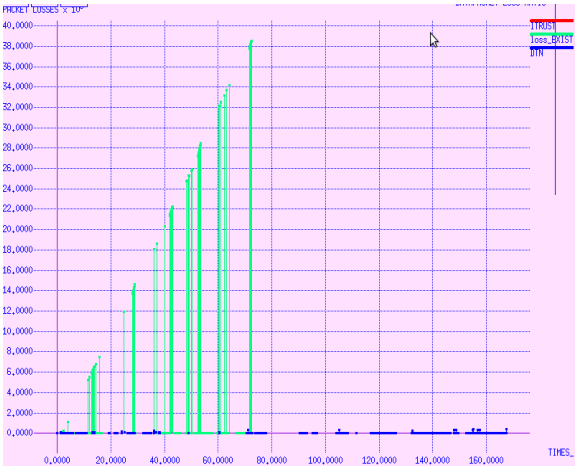

Fig 6: Data Packet Loss Rate

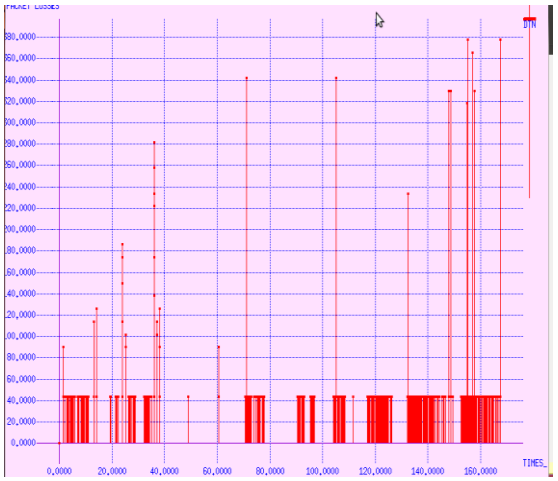

Fig 7: Comparison Graph Of Data Packet Loss Rate

C**.***DELAY RATIO:*

It shows the delay ratio of the proposed algorithm.The average delay between sending of the data packet by CBR source and its receipt at the corresponding CBR receiver. Delay time will reduce through the geographic routing protocol.ZRP protocol will be the centralized architecture, its suffers to collect the information about the all nodes in the network. We have taken existing system that features Direct and Indirect Trust alone for detection of malicious node without Certificate Authority and Fuzzy Logic.

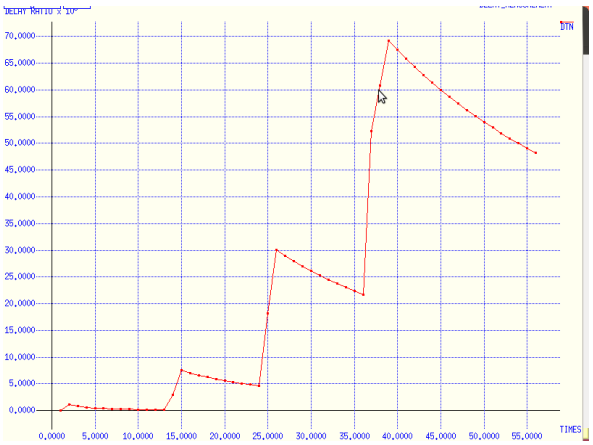

Fig 8: Delay Measurement

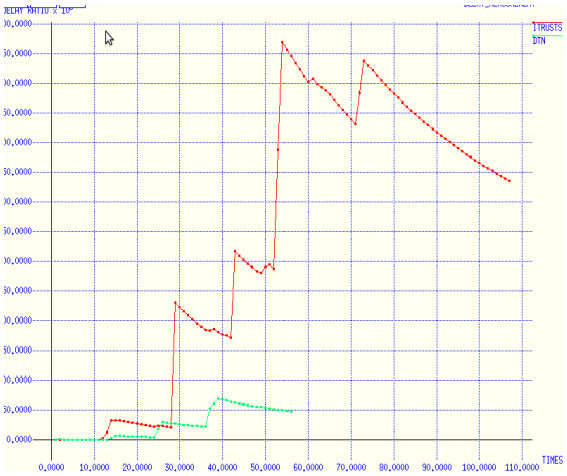

Fig 9: Comparison Graph Of Delay Measurement

A. PROTOCOL THROUGHPUT:

It shows the throughput of proposed algorithm.Fuzzy algorithm used to simulate the results of performance analysis while compare to the RSA algorithm.DTN protocol achieves the effectiveness and efficiency of the simulation results than the ZRP protocol. Data are collected from the existing system node and the probability of

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

detecting misbehaving nodes is compared with the probability rate of proposed system. The trust values of the nodes that fall below the threshold are assumed to be malicious.

Fig 10: Protocol Throughput

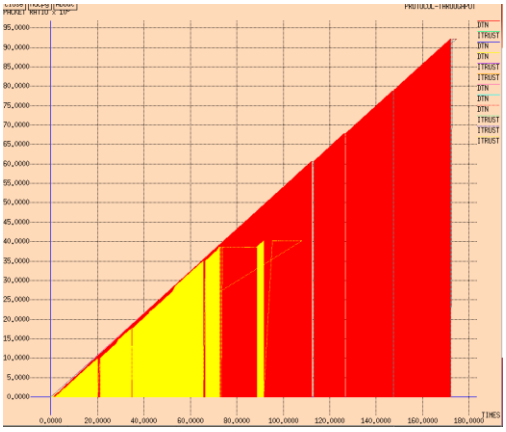

Fig 11: Comparison Graph Of Protocol Throughput

As a simulation result its achives the packet delivery ratio,total loss rate,delay ratio, throughput, channel measurement, protocol frequency,source signal strength and destination signal strength frequency.Through simulation result its detect the malicious node as 0.5%. By techinque Of MIMO its reduces the data loss rate and frequently a secure data reaches to the destination by the DTN routing protocol.While the comparison of existing and proposed system the better result achives in the proposed system.

V.CONCULSION AND FUTURE WORK

MANET consists of various mobile devices with different performance capabilities. During deployment, security emerges as a central requirement due to many attacks that affects the performance of the ad hoc networks. The proposed work will offer a healthy network by considering the distinctive features like mobility, security and quality of service. Trust is assigned to all the mobile nodes considering the available energy and the nodes are clocked and time lined. Fuzzy Logic based on Certificate Authority will provide secure way of message exchanges. Integrated approach of Trust and Fuzzy logic based DTN protocol will secure the communication. In this paper, we analyse the problem of black hole attacks in ZRP routing protocol in network. We proposed a fuzzy system to detect the black hole attack on the DTN protocol. We simulated our proposed solution using the NS-2.35 simulator and compared the performance in terms of packet delivery ratio, Data loss rate, protocol frequency, throughput, channel measurement and delay. Our system not only detects the black hole attack and also isolates black hole from the network. In this section, future work of this project will be discussed. It is still needed to improve the performance of routing protocol and to detect the malicious node in the network. We may use the WIMAX perimeter stateless routing protocol improves the routing performance.

REFERENCES

[1] A. Amuthan, B.Aravind Baradwaj" Secure Routing Scheme in MANETs using Secret Key Sharing
[2] Jiaheng Wang, Member, IEEE, Gesualdo Scutari, Member, IEEE, and Daniel P. Palomar, Senior Member, IEEE," Robust MIMO Cognitive Radio Via Game Theory".

[3] Atekeh Maghsoudlou, Marc St-Hilaire, and Thomas," A Survey on Geographic Routing Protocols for Mobile Ad hoc Networks".

[4] Yuvraj Singh and Sanjay Kumar Jena," Intrusion Detection System for Detecting Malicious Nodes in Mobile Ad hoc Networks".
[5] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks," IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858- 3868, Oct. 2008.
[6] Mareeswari V, Ramakrishna K and Vijayan R,(2011) "Energy based Trust solution for Detecting Selfish Nodes in MANET using Fuzzy logic", International Journal of Research and Reviews in Computer Science (IJRRCS) , Vol. 2, No. 3.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

[7] Priyambada Sahu, Sukant Kishoro Bisoy, Soumya Sahoo" Detecting and Isolating Malicious Node in AODV Routing Algorithm "International Journal of Computer Applications (0975 – 8887) March 2013.
[8] R. Lu, X. Lin, H. Zhu, and X. Shen, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.
[9] Ahmad Ridha, Ali Rizvi, Farag Azzedin,(2007) "Fuzzy Trust for Peer-to-Peer Based Systems", World Academy of Science, Engineering and Technology.
[10] E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay-Tolerant Networks," Proc. Military Comm. Conf. (Milcom '10), 2010.
[11] D. Fudenberg and J. Tirole, Game Theory. MIT Press, 1991.
[12] A.Rajaram and Dr.S.Palaniswami , (2010) "A High Certificate Authority Scheme for Authentication in Mobile Ad hoc Networks", IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No 5

BIOGRAPHY

S.KARTHIKA has completed her graduation in B.E Electronics and Communication Engineering in the year 2010 at Ranippettai engineering College, Vellore affiliated to Anna University, Chennai, India and presently doing her post graduation in M.E Applied Electronics in the year 2013-15 at Kingston Engineering College, Vellore. She is working towards her research in the field of Mobile adhoc network. Her area of Specialization includes wireless network and VLSI design.