ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

An Efficient Protection against Collaborative Attacks in Manet Using Cooperative Bait Detection Scheme

B. Kondaiah[1], Dr. M. Nagendra[2]

Research Scholar, Dept. of CST, Sri Krishnadevaraya University, Anantapur, India[1]

Associate Professor, Dept. of CST, Sri Krishnadevaraya University, Anantapur, India [2]

ABSTRACT: Mobile Ad Hoc Networks (MANETs) are formed dynamically by an autonomous system of nodes that are connected via wireless links without using the existing network infrastructure. One of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. In the presence of malicious nodes, this requirement may lead to serious security concerns for instance; such nodes may disrupt the routing process. In this context, preventing or detecting malicious nodes launching collaborative black hole , gray hole or wormhole attacks is a challenge. This paper attempts to resolve this issue by designing an Adhoc on demand distance vector (AODV) based routing mechanism, which is referred to as the cooperative bait detection scheme (CBDS), that integrates the advantages of both proactive and reactive defense architectures. Our CBDS method implements a reverse tracing technique to help in achieving the stated goal. Simulation results are provided, showing that in the presence of malicious-node attacks.

KEYWORDS: MANET, Cooperative bait detection scheme (CBDS), Adhoc on-demand distance vector (AODV), Collaborative black hole attacks, Gray hole attacks, Wormhole attack.

I. INTRODUCTION

Mobile ad hoc networks (MANETs) [1] have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure flesh property. In a MANET, each node not only works as a host, but can also act as a router. While receiving data, nodes also need cooperation with each other to forward the data packets, thereby forming a wireless local area network [3]. These great features also come with serious drawbacks from a security point of view. Indeed, the aforementioned applications impose some stringent constraints on the security of the network topology, routing, and data traffic. For instance, the presence and collaboration of malicious nodes in the network may disrupt the routing process, leading to a malfunctioning of the network operations.

II. RELATED WORK

Jian-Ming Chang,Po-Chun Tsou, IEEE [2014]. In this paper tries to solve the issues of blackhole and grayhole attacks caused by malicious nodes by designing a Dynamic Source Routing (DSR) mechanism known as Cooperative Bait Detection Scheme (CBDS). It combines the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio. It achieves its goal with Reverse tracing technique. Cooperative Bait Detection scheme is proposed to detect malicious nodes in Manet for the grayhole and blackhole attacks. Cooperative Bait Detection Scheme (CBDS) has been used to tackle blackhole and grayhole attacks caused by malicious nodes [1]. CBDS combines the advantages of both proactive and reactive detection schemes to detect malicious nodes as proactive detection scheme monitors nearby nodes and avoiding attacks in initial stage and reactive detection scheme triggers only when detection node detects significant drop in delivery ratio. It achieves its goal with Reverse tracing technique.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

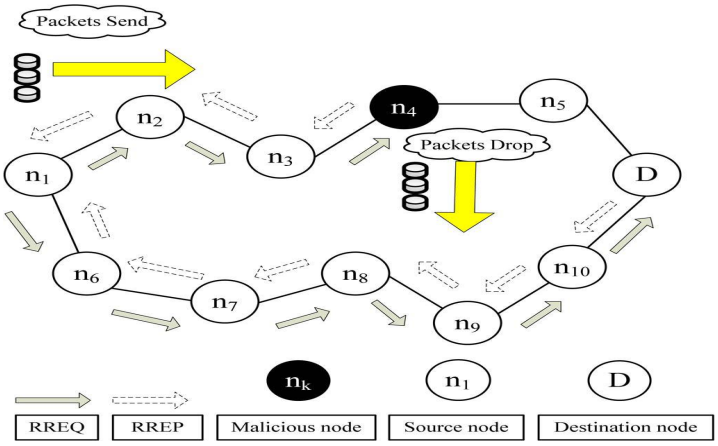


Fig. 1. Black hole attack–node *n*4 drops all the data packets.

Many research works have focused on the security of MANETs. Most of them deal with prevention and detection approaches to combat individual misbehaving nodes. In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network. The lack of any infrastructure added to the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as a black hole (known as variants of black hole attacks). In black hole attacks (see Fig. 1), a node transmits a malicious broadcast informing that it has the shortest path to the destination, with the goal of intercepting messages.

In gray hole attacks, the malicious node is not initially recognized as such since it turns malicious only at a later time, preventing a trust-based security solution for detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it.

In a wormhole attack, an attacker receives packets at one end point in the network, tunnel data packets to another endpoint in the network, and then replays them into the network from that point. This tunnel between these end points cause two colluding attacks is known as a wormhole.

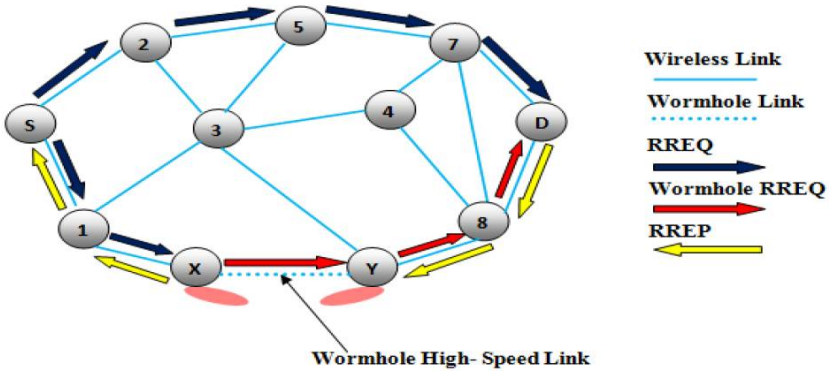


Fig 2: Wormhole Attack

In the above Fig. 2**,** the nodes “X” and “Y” are malicious node that forms the tunnel in the network. The source node “S” when initiates the RREQ message to find the route to node “D” destination node. The immediate neighbor node of source node “S”, namely “2” and “1” forwards the RREQ message to their respective neighbor “5” and “X”. The node “X” when receive the RREQ its immediately share with it “Y” and later it initiates RREQ to its neighbor node “8”, through which the RREQ is delivered to the destination node “D”. Due to high speed link, it forces

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

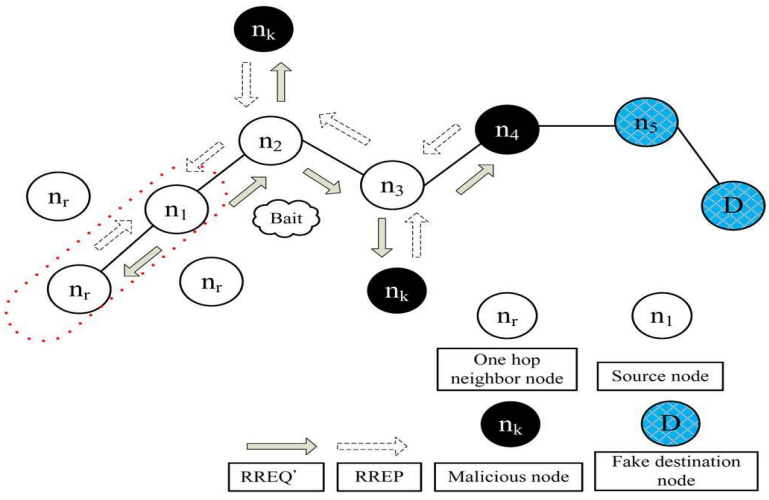
the source node to select a route <S-1-8-D> for the destination. It results in ignoring RREQ that arrives at a later time and thus invalidates the legitimate route <S-2-5-7-D>. The communication done by <S-1-8-D> is thereby listened by the wormhole nodes "X" and "Y". So the wormhole nodes and their high speed link pose a major security threat to the network.

In this case, a malicious node (so-called black hole node) can attract all packets by using forged Route Reply (RREP) packet to falsely claim that "fake" shortest route to the destination and then discard these packets without forwarding them to the destination. In this paper, our focus is on detecting collaborative black hole, gray hole/wormhole attacks using an ad hoc on demand distance vector (AODV)-based routing technique.

III. PROPOSED APPROACH:

In This paper proposes, the Cooperative bait detection scheme (CBDS), which aims at detecting and preventing malicious nodes launching collaborative black hole ,Gray hole/Wormhole attacks in MANETs. In our approach, the source node selects an adjacent node with which to cooperate, in the sense that the address of this node is used as a bait destination address to bait hostile nodes to send a reply RREP message. Hostile nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again. The CBDS scheme merges the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps in order to reduce the resource wastage.

CBDS architecture



The CBDS scheme comprises three steps:

1) Initial Bait Step 2) The Reverse tracing step 3) The Shifted to reactive defense step

Initial Bait:

The goal of the bait phase is to entice a malicious node to send a reply RREP by sending the bait RREQ that it has used to advertise itself as having the shortest path to the node that detains the packets that were converted. To achieve this goal, the following method is designed to generate the destination address of the bait RREQ .The source node stochastically selects an adjacent node, within its one-hop neighborhood nodes and cooperates with this node by taking its address as the destination address of the bait RREQ. First, if the neighbor node had not launched a black hole

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

attack, then after the source node had sent out the RREQ , there would be other nodes' reply RREP in addition to that of the neighbor node. This indicates that the malicious node existed in the reply routing. The reverse tracing program in the next step would be initiated in order to detect this route. If only the neighbor node had sent the reply RREP, it means that there was no other malicious node present in the network and that the CBDS had initiated the AODV route discovery phase.

The Reverse Tracing:

The reverse tracing program is used to detect the behaviors of malicious nodes through the route reply to the RREQ message. If a malicious node has received the RREQ, it will reply with a false RREP. Accordingly, the reverse tracing operation will be conducted for nodes receiving the RREP, with the goal to deduce the dubious path information and the temporarily trusted zone in the route. It should be emphasized that the CBDS is able to detect more than one malicious node simultaneously when these nodes send reply RREPs.

The Shifted to Reactive defense step:

After the above initial proactive defense (steps 1 and 2), the AODV route discovery process is activated. When the route is established and if at the destination, it is found that the packet delivery ratio has significantly falls to the threshold, the detection scheme would be triggered again to detect for continuous maintenance and real-time reaction efficiency The threshold is a changing value in the range that can be adjusted according to the current network efficiency.

IV. PERFORMANCE EVALUATION

The NS2 simulation tool is used to study the performance of our CBDS scheme. We employ the IEEE 802.11 MAC with a channel data rate of 11 Mb/s. In our simulation, the CBDS is set as dynamic threshold. All remaining simulation parameters are captured in Table I. We randomly select the malicious nodes to perform attacks in the network.

Performance metrics

We have compared the CBDS against the AODV on the basis of following performance metrics.

Packet Delivery Ratio: This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. Here, *pktdi* is the number of packets received by the destination node in the *i*th application, and *pktsi* is the number of packets sent by the source node in the *i*th application. The average packet delivery ratio of the application traffic *n*, which is denoted by *PDR*, is obtained as

$$PDR = \frac{1}{n}\sum_{i=1}^{n}\frac{pktd_i}{pkts_i}.$$

Throughput: This is defined as the total amount of data (b_i) that the destination receives them from the source divided by the time (t_i) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput of the application traffic n. which is denoted by T, is obtained as

$$T = \frac{1}{n}\sum_{i=1}^{n}\frac{b_i}{t_i}.$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

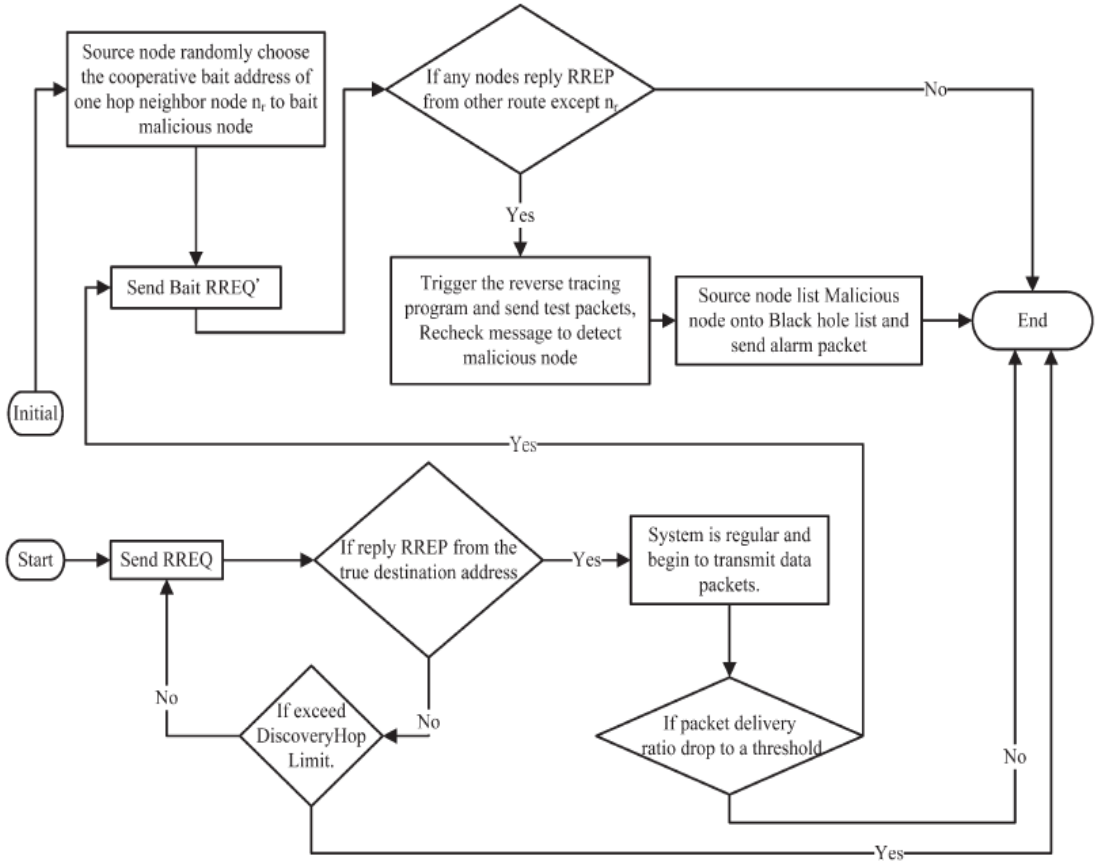


Fig 3. Operation of CBDS

TABLE – II

SIMULATION PARAMETERS	
Parameter	Value
Application Traffic	10CBR
Transmission rate	4 packets/s
Radio range	250m
Packet Size	512 bytes
Channel data rate	11 Mbps
Pause time	0s
Maximum Speed	20m/s
Simulation time	800s
Number of Nodes	50
Area	700m*700m
Malicious nodes	0% 40%
Threshold	Dynamic Threshold

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Two simulation scenarios are considered:

1) Scenario 1: Changing the percentage of malicious nodes with a fixed mobility.
2) Scenario 2: Changing the mobility of nodes under fixed percentage of malicious nodes.

Under these scenarios, we study the effect of different thresholds of the CBDS on the aforementioned performance parameters. The results are as follows.

Changing the percentage of malicious nodes with fixed mobility

We study the packet delivery ratio of the AODV and CBDS for thresholds when the percentages of malicious nodes in the network vary from 0% to 40%, the maximum speed of nodes is set to 20 m/s.

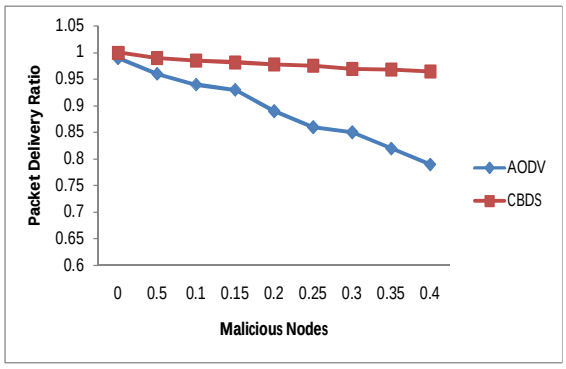


Fig 3 :Packet delivery ratio of AODV and CBDS

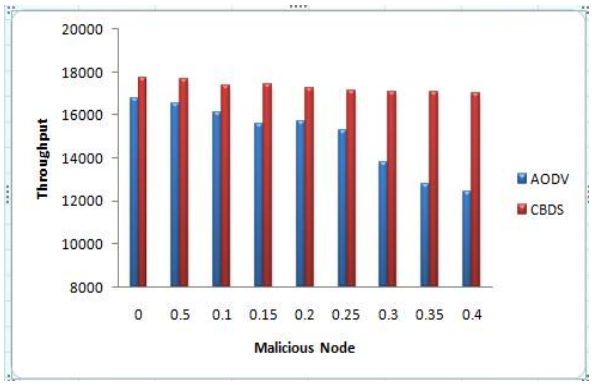


Fig 4: Throughput of AODV and CBDS

We compare AODV and CBDS in terms of packet delivery ratio and throughput when the malicious nodes increase in the network. Here the threshold for the CBDS is set to the dynamic threshold value. Even the network is relatively high (up to 40%), it is observed that the CBDS can still detect malicious nodes successfully while keeping the throughput above 15000 bit/s. The result packet delivery ratio and throughput compared in Fig.3 and Fig.4 respectively.

In Fig.3 It can also be observed that AODV heavily suffers from increasing black hole and wormhole attacks since does not have any detection and protection mechanism to prevent above attacks. Moreover, the packet delivery ratio of the CBDS is highest compared with that of AODV routing protocol.

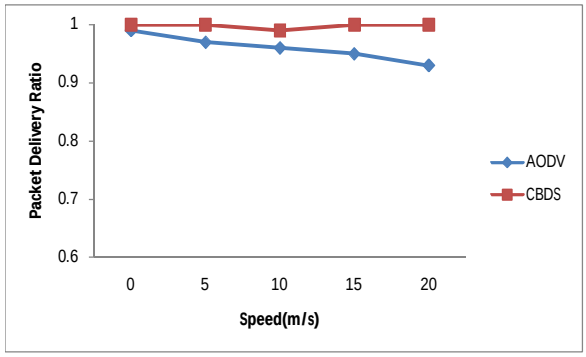


Fig 5: Packet delivery ratio on AODV and CBDS, Under varying node speed

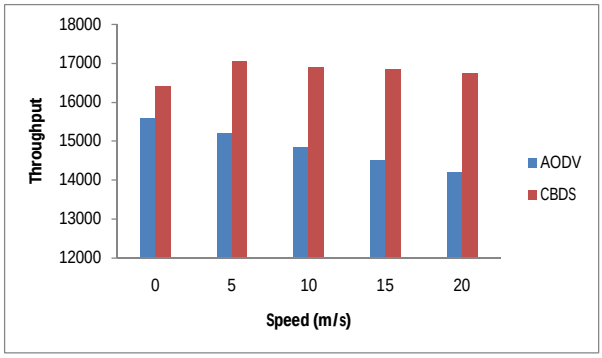


Fig 6: Throughput on AODV and CBDS, under varying node speed

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 2, February 2016

Changing the mobility of nodes under a fixed percentage of malicious nodes

In this scenario, the maximum speed of nodes is varied from 0 to 20 m/s, and the percentage of malicious nodes is fixed 20%. We study the packet delivery ratio are captured in Fig 5. It can also be observed that the packet delivery ratio of AODV and CBDS. Slightly decreases when the nodes speed increases. The CBDS yields a higher packet delivery ratio compared with AODV.

We study the Throughput of the AODV and CBDS. The results captured in Fig 6. It can be observed that the throughput of AODV and the CBDS Slightly decreases when the nodes speed increases. The CBDS yields the higher throughput compared with AODV in all cases.

V. CONCLUSION AND FUTUREWORK

In this paper, we have proposed a new mechanism is known as CBDS for detecting malicious nodes in MANETs under Collaborative black hole, gray hole/wormhole attacks. In our simulation result revealed that the CBDS outperforms the AODV routing. The CBDS packet delivery ratio and throughput is very high than AODV. As future work, we intended to investigate the integration of the CBDS with other well-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against attacks.

REFERENCES

1. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, han-Chieh Chao, and Chin-Feng Lai, Member,IEEE, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Scheme",1932-8184 ©2014 IEEE.
2. C.E Perkins and E.M. Royer. Ad-hoc On-Demand Distance Vector Routing. Proceeding of the 2nd IEEE Workshop on mobile Computing systems and Applications, pages 90-100.New Orleans, L.A.February 1999
3. Yang H, Lou H, Ye F, Lu S, Zhang L (2004) Security in Mobile Ad Hoc Networks: Challenges and Solutions. IEEE Wireless Communications 11(1):38–47. doi: 10.1109/MWC.2004.1269716
4. P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in *Proc. 2nd Intl. Conf. Wireless Commun., VITAE*, Chennai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.
5. S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013). [Online]. Available: http://www.elook.org/computing/rfc/rfc2501.html
6. C. Chang, Y. Wang, and H. Chao, "An efficient Mesh-based core multicast routing protocol on MANETs," *J. Internet Technol.*, vol. 8, no. 2, pp. 229–239, Apr. 2007.
7. D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.
8. I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in *Proc. IEEE Aerosp. Conf.*, 2002, vol. 6, pp. 2727–2740.
9. A. Baadache and A. Belmehdi, "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.
10. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265.
11. K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," *Int. J. Comput. Appl.*, vol. 1, no. 22, pp. 28–32, 2010.
12. H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002.
13. S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in *Proc. Int. Conf. Wireless Netw.*, Jun. 2003, pp. 570–575.
14. H. Weerasinghe and H. Fu, "Preventing cooperative blackhole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in *Proc. IEEE ICC*, 2007, pp. 362–367.

BIOGRAPHY

B. Kondaiah is a Research scholar of Computer Science and Technology Department, in Sri Krishnadevaraya University. He received Master of Computer Science(MSc) degree in 2008 from S.K University, Anantapur, Andhra Pradesh. His research interests are Computer Networks(Wireless Ad hoc Networks).