Scientific Journal of Impact Factor (SJIF): 4.14

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 3, Issue 8, August -2016

A Novel approach to prevent Collaborative Black Hole attacks in MANETS using Cooperative Bait detection Scheme (CBDS)

Sharath Chandrahasa K C[1], K R Prasannakumar[2],

[1]*Final year student, M.Tech. (Computer Networks), SIT College, Karnataka, India*
[2]*Assistant Professor, Department of Computer Science and Engineering, SIT College, Karnataka, India*

Abstract - *This paper presents a detail description of novel approach for collaborative attacks in Mobile Ad hoc Networks (MANETs). Providing secure communication is one of important aspects In Mobile Ad hoc Networks (MANETs). Routing protocols helps to transfer the packets from source to destination. Routing Protocols are vulnerable to collaborative black hole attacks. When malicious nodes work together to drop the packets called collaborative attacks, i.e. Blackhole attacks completely drops the packets in MANETs. We propose a Cooperative Bait detection (CBDS) mechanism for prevent collaborative black hole attacks in MANETs. In this scheme integrates features of Dynamic Source Routing (DSR) and 2ACK protocols. CBDS scheme merges the advantage of both proactive and reactive defense architecture and provide secure data transmission using key distribution center (KDC). In the initial stage it uses Bait id concept to detect malicious node in the network using proactive architecture, and it switches to reactive defense strategy. The scheme involves three steps, the bait step, suspected path detection and the Confirmation Request. The bait step attracts the malicious node and next step detect suspected path. The last step involves the confirmation of the given path is secure for the destination request from its neighbor. To secure data transmission we use RSA decryption and encryption algorithm scheme. The CBDS outperforms the DSR, 2ACK, and best-effort fault-tolerant routing (BFTR) protocols chosen as benchmarks in terms of packet delivery ratio and routing overhead chosen as performance metrics.*

***Key Words*:** *DSR, 2ACK, CBDS, Black hole, MANET, BFTR*

1. INTRODUCTION

A mobile ad-hoc (MANET) network is made up of group of mobile nodes, which cooperates to communicate with each other without any fixed central base station [1]. A mobile ad hoc network (MANET), sometimes called a mesh mobile network, is a network of mobile devices connected by wireless links. MANET is a kind of point to point transmission type and is a group of mobile nodes communicating with each other by wireless [2]. Due to infrastructure-less nature of the network, routing and network management is done cooperatively by the nodes i.e. the nodes themselves maintains the functioning of the network [3] [4]. The topology of the network varies rapidly and unpredictable over time because of the mobility of the nodes. The lack of any infrastructure, mobile nodes are dynamically changing the network topology in infrastructure less network makes MANET more vulnerable to various types of routing attacks than a typical wireless network. The attacker would perform different types of attacks such as Black hole and Collaborative. DSR [5] involves two main processes: route discovery and route maintenance. To execute the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the network. If an intermediate node has routing in-formation to the destination in its route cache, it will reply with a RREP to the source node. When the RREQ is forwarded to a node, the node adds its address information into the route record in the RREQ packet. When destination receives the RREQ, it can know each intermediary node's address among the route. The destination node relies on the collected routing information among the packets in order to send a reply RREP message to the source node along with the whole routing information of the established route. DSR does not have any detection mechanism, but the source node can get all route information concerning the nodes on the route. In our approach, we make use of this feature.

1.1 Blackhole attack

: In blackhole 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 this case, a malicious node (so-called blackhole 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.

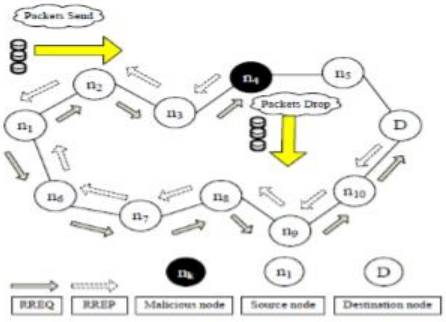


Figure 1. Black hole attack. Node n_4 drops all packets

1.2 Cooperative black: Cooperative black hole (see fig.2) attacks mean several malicious nodes cooperate with each other and work just like a group. This kind of attack results in many detecting methods fail and causes more immense harm to all network [11].

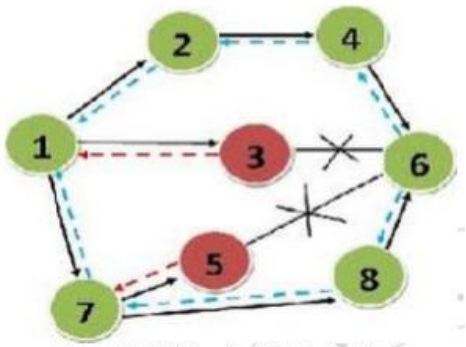


Figure 2: Collaborative Blackhole Attack

2 RELATED WORK

A number of researches are being carried for enhancing the security in Manet. Since there is no particular line of defense, security for manet is still a major concern for man. Some of the researches for the detection of blackhole attack are given. Kozma, and L.Lazos, "REAct: resource-efficient for node misbehavior in ad hoc networks based on random audits," [6] Based on Audit Procedure. When destination node detects a heavy packet drop, it triggers the source node to initiate the audit procedure. Source node chooses an audit node and it generates behavioral proof. Similarly source node prepares it behavioral proof .On the basis of comparison of results malicious nodes are detected. Drawback was that it is a reactive approach. Only if there is a drop in packet delivery ratio, the mechanism is triggered. Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala," A Review of Current Routing Attacks in Mobile Ad Hoc Networks," [7] Introduced the concept of route request (RREQ) and route reply (RREP) to avoid the blackhole attack. The intermediate node along with RREPs sends RREQs to its next-hop node toward the destination node. After receiving a RREQ, the next-hop node checks in its cache for a route to the destination. If it has the route, it sends the RREP to the source. Upon receiving the RREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in RREP. If both are matched, the source node judges that the route is correct. It was dependent on the intermediate nodes reply. Also it was able to detect only single black hole.W. Wang, B.Bhargava, and M. Linderman, "Defending against Collaborative Packet Drop Attacks on MANETs," [8] Introduced the approach of hash based function in REAct system. Enabled the data traffic and forward path detail available in behavioral proof. Upon drop in the packet delivery ratio initiates the blackhole detection. Based on the reactive detection. Latha Tamilselvan and Dr. V Sankaranarayanan," Prevention of Co-operative Black Hole Attack in MANET"[9] designed an approach for detection of co-operative black hole attack, based on the Fidelity table where presence of 0 indicates a malicious node. But it failed for the case of DSR. Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria," Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol" [10] proposed a simple scheme which depends on the details of intrusion detection from local nodes rather than from the source node. This scheme is used only for the case of AODV as it has the advantage of sequence number.

3 PROPOSED APPROACH

The DSR based secure routing protocol that we are using detects and avoids the black hole attack. CBDS (Cooperative Bait detection scheme) uses the concept of sending bait id and attracts black hole to reply the fake routing information. Initially it sends a virtual and random address as its destination address. Proactive detection is used initially. In case presence of any malicious node is detected, it is included in the black hole list. We use the proactive detection only in initial stage. There by

reducing the routing extra overhead. As soon as the initial stage is over, it becomes reactive detection. Normal packet transmission takes place.

Upon the completion of the process it checks the packet delivery ratio. If drop in packet delivery ratio is found, destination node sends alarm to the source which triggers the black hole detection. Our mechanism merges the advantage of proactive detection in the initial stage followed by superiority of the reactive detection. In CBDS scheme the packet format of the RREP and RREQ is modified. In case of DSR routing, the source will have all the information about the intermediate nodes participating in its mechanism. Upon the reception of the RREP, it will know details of the nodes participating in packet transmission but it will not know exactly which the malicious node is. The packet format of RREP is modified such that Reserved field is used as Record address. The record address enables to trace the malicious node. In addition it has RREQ" packet which has a virtual and nonexistent address as its target address. Route discovery is initiated with the source sending RREQ" to all the nearby nodes. The target address of the RREQ" is a fake id i.e. a virtual non-existing random id is given .When a malicious node receives RREQ", it replies itself as the shortest path to the destination. Upon the reception of the RREP, from the record address field, the source will know which the malicious node is and removes it from its network, in its initial stage. Thus the malicious node is detected and is recorded in the blackhole list. Thus the proactive detection detects the presence of blackhole. Also all the nodes are made aware of the blackhole.

The proactive detection makes use of the record address and the false id to perform the detection of the malicious node. Upon detection of the malicious node it is removed from the network by triggering alarm to all the nodes in the network about the malicious node. Thus future responses from the malicious nodes are discarded. After the initial proactive stage, it becomes reactive detection. Source sends the route RREQ to the nearby nodes. The intermediate node sees to the target address. If it is the shortest path to the destination it adds its address to the field and forwards the packet to the destination. In case it has already received the packet it just discards the packet. If it is the target address it sends RREP to the source and normal packet transmission starts. Upon the completion of the process, the destination checks the packet delivery ratio. CBDS scheme uses the advantage of both the proactive and the reactive detection. In the initial stage it reduces the chance of malicious node. In later stage it becomes reactive detection thereby reducing the overhead

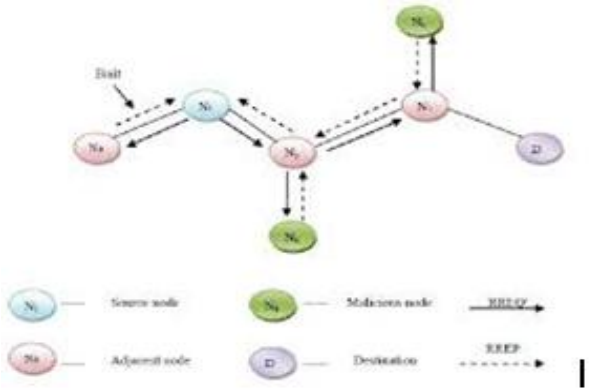
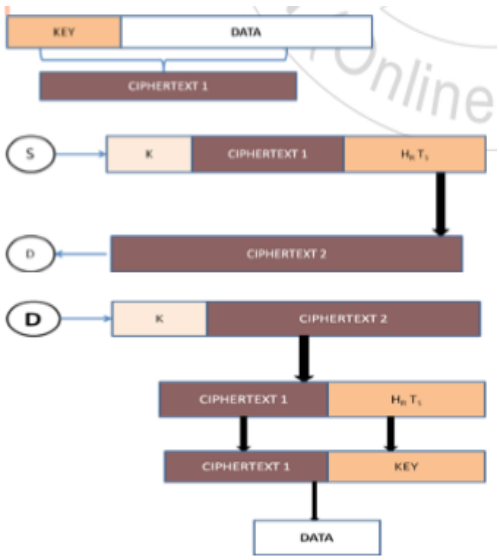


Figure 3: Operation of CBDS

The Cooperative bait detection approach detects the malicious nodes that attempt to launch collaborative blackhole attacks. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a blackhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of CBDS lies in the fact that it integrates the proactive and reactive defense architectures to achieve the aforementioned goal.

3.1 Secure Data Transmission: To allow secure data transmission after the detection of black hole attack. The Key Distribution Center (KDC) provides key „K" which is shared between source and the destination .Source generates the key KEY, using number of hops (HR) involved in the route and message sent time (TS). Using KEY data is encrypted at the first level and generates Ciphertext1. In the second level, Ciphertext1 ,TS and HR are encrypted using K , In the second level before encrypting the TS and HR , they should be shuffled using some shuffling algorithm. The Ciphertext2 is sent to the destination ,The destination makes use of K and decrypt the Ciphertext2 by making use of shuffling algorithm, destination obtains values of TS and HR .Using TS and HR, destination generates KEY using KEY, Ciphertext1 is decrypted.



4 PERFORMANCE EVALUTION

The proposed work is simulated using NS-2 software. Performance is evaluated using performance metrics such as Packet Delivery Ratio, Routing Overhead and Throughput. The results are based on the implementation of the Cooperative Bait Detection Scheme. The results shown below are comparison graphs of 2ACK, DSR protocol and the ECBDS in presence of malicious node for the performance parameters.

4.1 Performance Metrics

(A) Packet Delivery Ratio: This is defined as the ratio of the number of packets received at the destination and number of packets send by source. Fig. 5 shows the Packet Delivery Ratio (PDF) comparison of the existing 2ACK and DSR with the proposed system. The PDR of CBDS is better than 2ACK and DSR protocols.

$$PDR=1/n\sum (pktdi/pktsi)\ n\ i=1$$

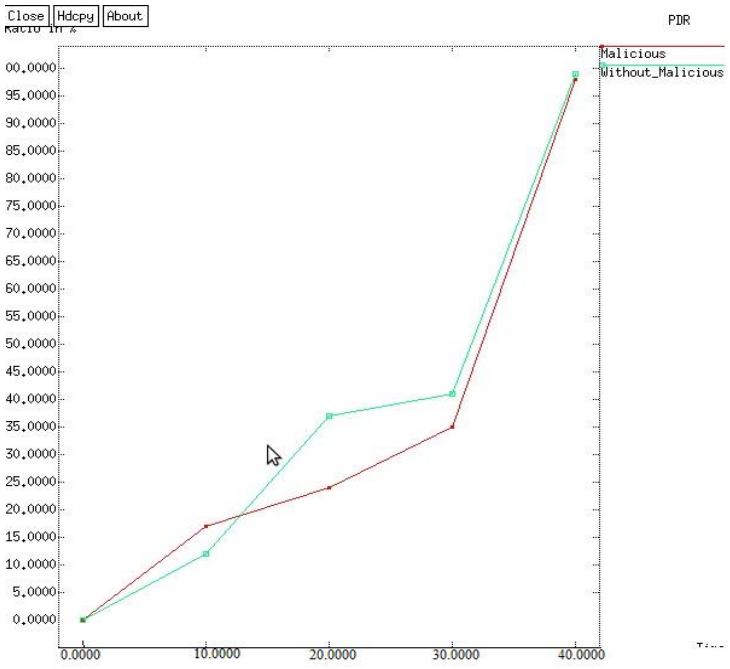


Figure 5: Packet Delivery Ratio

(B) Throughput: This is defined as the total amount of data that the destination receives them from the source. The throughput is the number of bits transmitted per second. Fig. 6 shows the Throughput comparison of the existing 2ACK, DSR with the proposed system. The Throughput of CBDS is better than 2ACK and DSR protocols

$$T=1/n\sum (bi/ti)\ n\ i=1$$

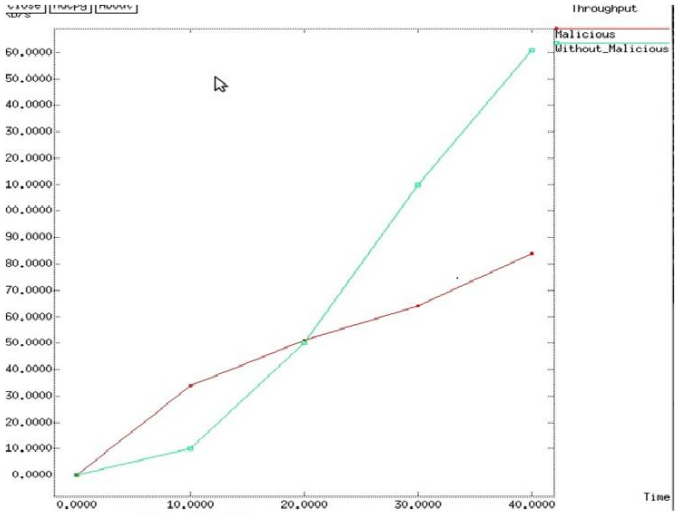


Figure 6: Throughput

(C) Routing Overhead: This metric represents the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. Fig. 8 shows the Routing Overhead comparison of the existing 2ACK, DSR with the proposed system. The Routing Overhead of CBDS is higher than 2ACK and DSR protocols. Because of encryption and decryption process in CBDS.

$$RO=1/n\sum (cpki/pkti)\ n\ i=1$$

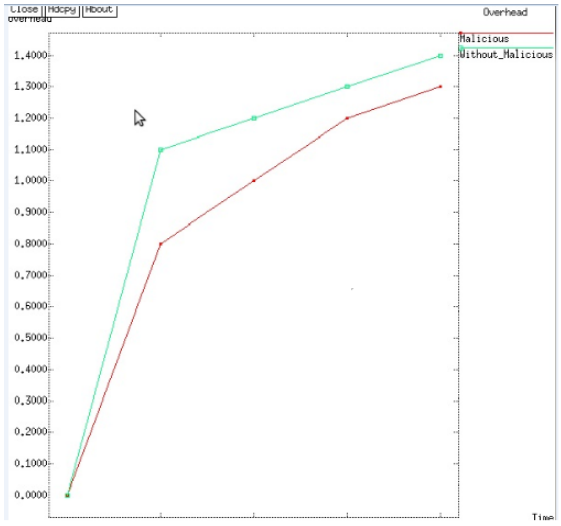


Figure 7: Routing Overhead

First, we tend to study the packet delivery quantitative relation of the BDS and DR for various thresholds once the share of malicious nodes within the network varies from third to five hundredth. The most speed of nodes is ready to 20m/s. Here, the edge price is ready to half of one mile, 96%, and also the action threshold, severally. The results capture in Fig. 6, may be ascertained that DR drastically suffers from blackhole attacks once the share of malicious nodes will increase. This can be attributed tothe actual fact that DR has no secure technique for detecting/ preventing blackhole attacks [4].

Our BDS theme shows the next packet deliverance quantitative relation compared there upon of DR. Even within the case wherever four-hundredth of the entire nodes within the network are malicious, the BDS theme still with success detects those malicious nodes whereas keeping the packet delivery quantitative relation higher than ninetieth. A threshold of ninety fifth would then end in earlier route detection than once the edge is eighty nine or is ready for the dynamic threshold price. Thus, the packet delivery quantitative relation once employing a threshold of ninety fifth is beyond that obtained once employing a threshold of eighty fifth or the dynamic threshold

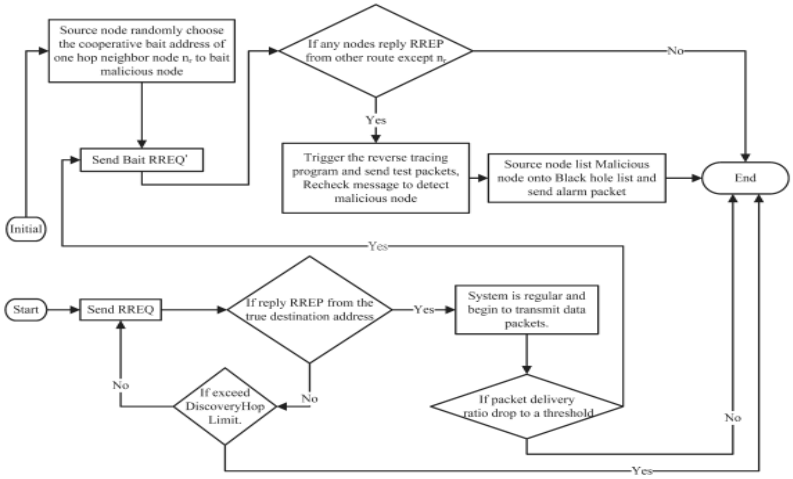


Figure 8: Flowchart of proposed work

Second, we tend to study the routing overhead of the BDS and DR for various thresholds. It may be ascertain that once the amount of malicious nodes will increase, DR produces all-time low routing overhead compared with the BDS. This can be attributed to the actual fact that DSR has no intrinsic security technique or defensive mechanism. In fact, the routing overhead created by the BDS for various thresholds may be a little beyond that created by DSR Consequently; Exchange ought to be created between routing overhead and packet delivery quantitative relation

5 PSEUDO CODE

Step 1: Send RREQ
Step 2: if (RREP == D true) \\ If RREP is from true destination
Step 3: system=1; \\ system is working fine
Step 4: else
Step 5: if (Time > T) \\ T is the discovery time threshold
Step 6: end process;
Step 7: else
Step 8: send RREQ again;
Step 9: end if
Step 10: end if
Step 11: if (PDR < T1) \\ if packet delivery ratio drops to a certain threshold
Step 12: Send Bait RREQ'
Step 13: else
Step 14: end process
Step 15: end if
Step 16: if (RREP == true) \\ if any RREP
Step 17: Trace Mechanism =1 ; \\ Trigger trace mechanism
Step 18: else
Step 19: end process;
Step 20: end if ;
Step 21: Initiate trace mechanism;
Step 22: MN detected;
Step 23: MN = black listed; \\ malicious is black listed

6 CONCLUSION

The CBDS detects and avoids the black hole attack in MANETS. It uses the proactive detection in its initial stage and reactive detection in the later stage. The proactive detection detects malicious nodes presence in the initial stage. The reactive detection reduces resource wastage. Secure data Transmission achieved using encryption and decryption process.

Performance of parameters such as Packet Delivery Ratio, Routing Overhead and Throughput. Compared to DSR ,A2K and CBDS offers a greater packet delivery ratio, Network Throughput is reduced. In future work, it can be extended for the reducing of Routing Overhead using integrated features of OSPF and RIP protocols.
The CBDS detects and avoids the black hole attack in MANETS. It uses the proactive detection in its initial stage and reactive detection in the later stage. The proactive detection detects malicious nodes presence in the initial stage. The reactive detection reduces resource wastage. Secure data Transmission achieved using encryption and decryption process. Performance of parameters such as Packet Delivery Ratio, Routing Overhead and Throughput. Compared to DSR ,A2K and CBDS offers a greater packet delivery ratio, Network Throughput is reduced. In future work, it can be extended for the reducing of Routing Overhead using integrated features of OSPF and RIP protocols.

REFERENCES

1. Vishnu K and Amos J Paul, "Detection and Removal of Cooperative Black/Gray Hol Attack I in Mobile ADHOC Networks", International Journal of Computer Applications, Vol. 1, No. 22, 2010.

2. Navdeep Kaur ,Mouli Joshi "Implementing MANET Security using CBDS for combat sleep Deprivation & DOS Attack" International Journal for science and Engineering.

3. Sudhir Agrawal, Sanjeev Jain and Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-hoc Networks", Journal of Computing, Vol. 3, ISSN 2151-9617, January 2011.

4. Po-Chun TSOU, Jian-Ming CHANG, Yi-Hsuan LIN, Han-Chieh CHAO and Jiann-Liang CHEN, "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", ICACT, Feb. 2011.

5. D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.

6. W.Kozma and L.Lazos,"REAct: resourceefficient accountability for node misbehavior in ad hoc networks based on random audits," in Proceedings of the Second ACM Conference on Wireless Network Security (WiSec), pp. 103- 110, 2009.

7. Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala," A Review of Current Routing Attacks in Mobile Ad Hoc Networks," International Journal of Computer Science and Security, volume (2) issue (3).

8. W.Wang, B.Bhargava, and M. Linderman, "Defending against Collaborative Packet Drop Attacks on MANETs," 28th International Symposium on Reliable Distributed Systems September 2009.

9. Latha Tamilselvan and Dr. V Sankaranarayanan," Prevention of Co-operative Black Hole Attack in MANET," Journal of Networks, VOL. 3, NO. 5, MAY 2008.

10. Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria," Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol," Australian Journal of Basic and Applied Sciences, 5(10): 1137-1145.

11. Fan-Hsun Tseng,li-Der Chou and Han_chieh Chao, "A survey of black hole/Collaborative black hole attacks in wireless mobile ad hoc networks," Humancentric and Information Sciences,1:4, 2011.

12. G.V.S.Raju and RehanAkbani, "Authentication in Wireless Networks", Proceedings of IEEE 40th Hawaii International Conference on System Sciences, 2007.

13. Radhika Saini and ManjuKhari, "Defining Malicious Behaviour of a Node and its Defensive Methods in Ad Hoc Networks", International Journal of Computer Applications, Vol. 20, April 2011

14. Ramandeep Kaur, Jaswinder Singh,"Towards Security against Malicious Node Attack in Mobile Adhoc Network", International Journal of Advance Research in Computer Science and Software Engineering, volume 3, issue 7, july 2013.

Authors Profile

Sharath Chandrahasa K C received the B.E degree in computer science and Engineering from VTU University in 2013 and currently pursuing final year M.Tech degree in Computer Networks Engineering in Siddaganga Institute of Technology Tumakuru**.**

K R Prasannakumar received the B.E. in Information Science and Engineering from VTU University and received M.Tech in Software Engineering from VTU University respectively. Currently working as a Assistant Professor in Computer science and Engineering Department, SIT college of Engineering, Tumakuru.

