



# INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

## A REVIEW ON SECURE ROUTING PROTOCOL IN MANET

RAVNEET KAUR T. BAGGA, DR. H.R DESHMUKH,

Dept. Of Computer Science & Engg., Dr. Rajendra Gode Institute of Technology & Research, Amravati.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

**Abstract:** 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. In this context, preventing or detecting malicious nodes launching grayhole or collaborative blackhole attacks is a challenge. This project attempts to resolve this issue by designing a dynamic source routing (DSR)-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, 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).

**Keywords:** Mobile ad hoc network (MANET), Cooperative bait detection scheme (CBDS), Dynamic source Routing (DSR), Collaborative blackhole attacks, Detection mechanism.



PAPER-QR CODE

Corresponding Author: MR. RAVNEET KAUR T. BAGGA

Access Online On:

[www.ijpret.com](http://www.ijpret.com)

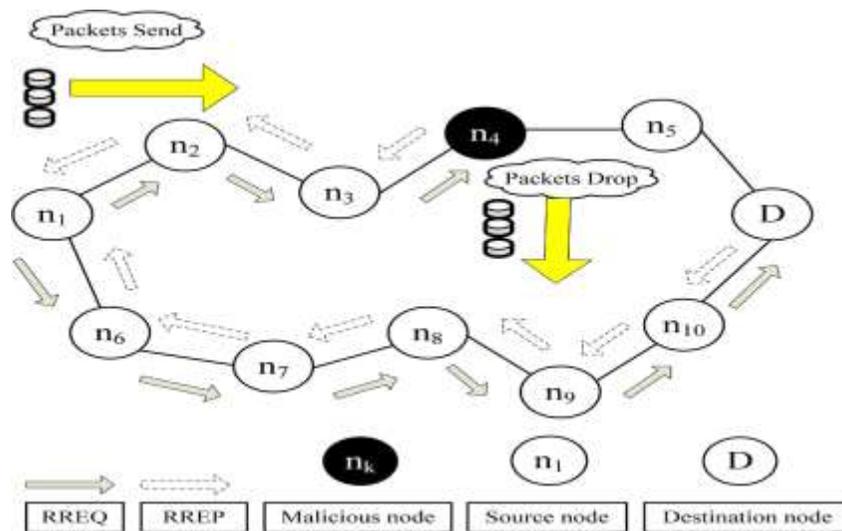
How to Cite This Article:

Ravneet Kaur T. Bagga, IJPRET, 2016; Volume 4(9): 1578-1584

## INTRODUCTION

DUE to the widespread availability of mobile devices, mobile ad hoc networks (MANETs) [1], [2] 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 infrastructureless 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. 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 with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks). 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. In grayhole 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 from detecting its presence in the network. It then selectively discards/forwards the data packets when packets go through it. In this paper, our focus is on detecting grayhole/collaborative blackhole attacks using a dynamic source routing (DSR)-based routing technique.



**Fig 1. Blackhole attack—node  $n_4$  drops all the data packets.**

DSR [4] 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 information 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. In this paper, a mechanism [so-called cooperative bait detection scheme (CBDS)] is presented that effectively detects the malicious nodes that attempt to launch grayhole/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.

## LITERATURE REVIEW AND RELATED WORK

Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost for detecting cooperative blackhole attacks. In addition, some of these methods require specific environments [5] or assumptions in order to operate. In general, detection mechanisms that have been proposed so far can be grouped into two broad categories.

1) Proactive detection schemes [6]–[12] are schemes that need to constantly detect or monitor nearby nodes. In these schemes, regardless of the existence of malicious nodes, the overhead of detection is constantly created, and the resource used for detection is constantly wasted. However, one of the advantages of these types of schemes is that it can help in preventing or avoiding an attack in its initial stage.

2) Reactive detection schemes [13]–[15] are those that trigger only when the destination node detects a significant drop in the packet delivery ratio.

Among the above schemes are the ones proposed in [9] and [13], which we considered as benchmark schemes for performance comparison purposes. In [9], Liu *et al.* proposed a 2ACK scheme for the detection of routing misbehavior in MANETs. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received. A parameter acknowledgment ratio, i.e., *Rack*, is also used to control the ratio of the received data packets for which the acknowledgment is required. This scheme belongs to the class of proactive schemes and, hence, produces additional routing overhead regardless of the existence of malicious nodes. In [13], Xue and Nahrstedt proposed a prevention mechanism called best-effort fault-tolerant routing (BFTR). Their BFTR scheme uses end-to-end acknowledgements to monitor the quality of the routing path (measured in terms of packet delivery ratio and delay) to be chosen by the destination node. If the behavior of the path deviates from a predefined behavior set for determining “good” routes, the source node uses a new route. One of the drawbacks of BFTR is that malicious nodes may still exist in the new chosen route, and this scheme is prone to repeated route discovery processes, which may lead to significant routing overhead. Our proposed detection scheme takes advantage of the characteristics of both the reactive and proactive schemes to design a DSR-based routing scheme able to detect grayhole/collaborative blackhole attacks in MANETs.

## PROBLEM ANALYSIS

The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks). In this project, a mechanism so-called cooperative bait detection scheme (CBDS) is presented that effectively detects the malicious nodes that attempt to launch grayhole/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.

## PROPOSED WORK & OBJECTIVE

This paper proposes a detection scheme called the cooperative bait detection scheme (CBDS), which aims at detecting and preventing malicious nodes launching grayhole/collaborative blackhole attacks in MANETs. In our approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. Malicious 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. Our 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.

The operations of the CBDS are captured in Fig. 2. It should be noticed that the CBDS offers the possibility to obtain the dubious path information of malicious nodes as well as that of trusted nodes; thereby, it can identify the trusted zone by simply looking at the malicious nodes reply to every RREP. In addition, the CBDS is capable of observing whether a malicious node would drop the packets or not. As a result, the proportion of dropped packets is disregarded, and malicious nodes launching a grayhole attack would be detected by the CBDS the same way as those launching blackhole attacks are detected.

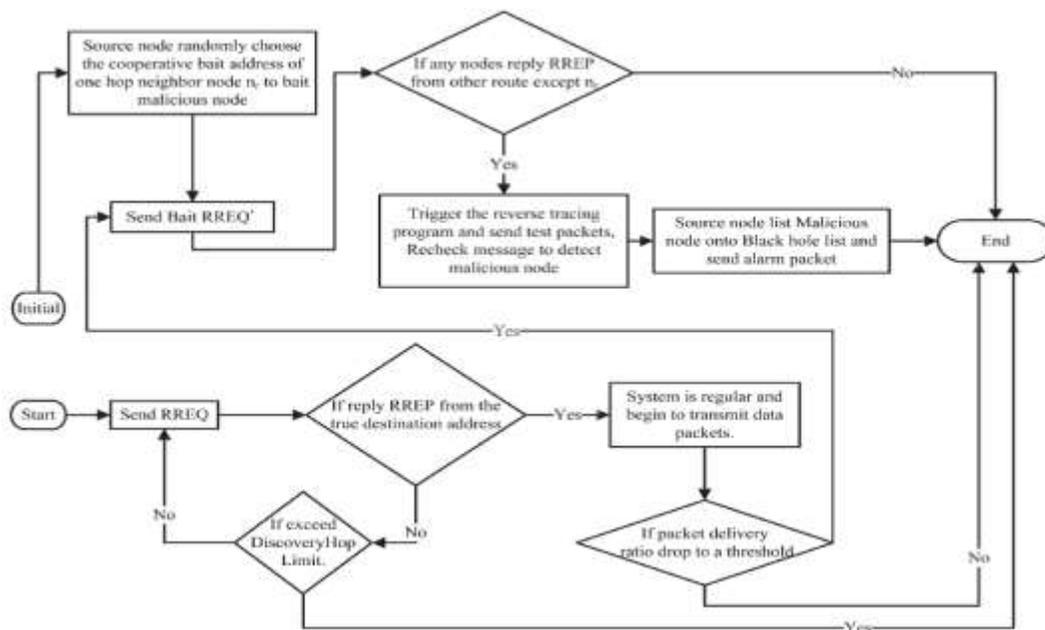


Figure 2: Operation of CBDS

## APPLICATION

1. Have been widely used for various important applications such as military
2. Crisis operations
3. Emergency preparedness and response

## A BENEFIT TO END USER

In mobile ad hoc networks (MANETs), a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other. In the presence of malevolent 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 grayhole or collaborative blackhole attacks is a challenge.

## CONCLUSION

In this paper, we have proposed a new mechanism (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative blackhole attacks. Our simulation results revealed

that the CBDS outperforms the DSR, 2ACK, and BFTR schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio. As future work, we intend to

- 1) Investigate the feasibility of adjusting our CBDS approach to address other types of collaborative attacks on MANETs and
- 2) 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 miscreants.

## REFERENCE

1. P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperativev bait detection scheme to prevent malicious node forMANET based onv hybrid defensev architecture," in *Proc. 2nd Intl. Conf. Wireless Commun., VITAE*, Chennai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.
2. S. Corson and J. Macker, RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations,vJan. 1999. (Last retrieved March 18, 2013). [Online]. Available: <http://www.elook.org/computing/rfc/rfc2501.html>
3. C. Chang, Y.Wang, and H. Chao, "An efficientMesh-based core multicast routing protocol onMANETs," *J. Internet Technol.*, vol. 8, no. 2, pp. 229–239, Apr. 2007.
4. D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Comput.*, pp. 153–181, 1996.
5. 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.
6. A. Baadache and A. Belmehdi, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," *Intl. J. Comput. Sci. Inf. Security*, vol. 7, no. 1, 2010.
7. S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in *Proc. 6th Annu. Intl. Conf. MobiCom*, 2000, pp. 255–265.
8. 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.
9. K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.
10. H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," *IEEE Commun. Mag.*, vol. 40, no. 10, Oct. 2002.