ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Co-operative Bait Detection Approach for Collaborative Packet Drop infiltration by Hostile Nodes of MANETs

Mrs. A. Naveena
Assistant Professor,
G. Narayanamma Institute of Technology & Science,
Hyderabad.

Dr. K. Rama Linga Reddy
Professor and HOD,
G. Narayanamma Institute of Technology & Science,
Hyderabad.

Abstract:

The fundamental requirement for the establishment of communication among nodes is that nodes should cooperate with each other. This also true for mobile ad hoc networks (MANETs), In the presence of malicious nodes, this requirement may lead to serious security concerns; for instance, such nodes may corrupt the routing process. In this context, prevention or detection of hostile nodes launching, may leads to gray hole or collaborative black hole attacks, which is a challenge for the existing system.

This paper written to resolve this issue by implementing 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 strategy to help in achieving the goal.

Simulation results are showing that in the presence of hostile-Node attacks, the CBDS outperform the DSR, and best-effort fault-tolerant routing (BFTR) protocols (select as benchmarks) in terms of packet delivery ratio and routing overhead (select as performance metrics).

Index Terms:

Cooperative bait detection scheme (CBDS), collaborative bait detection, collaborative black hole attacks, detection mechanism, dynamic source routing (DSR), gray hole attacks, hostile node, mobile ad hoc network (MANET).

I.INTRODUCTION:

The universal availability of mobile devices creates mobile ad hoc networks (MANETs) [1], [2] which have been widely used for various important and secure applications such as military crisis operations and emergency preparedness and response operations. This is primarily due to their infrastructure less property. In a MANET, individual node not only works as a host but can also behave as a router. On receiving data, nodes also need cooperation with each other to send 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 hostile nodes in the network may corrupt the routing process, causes the malfunctioning of the network operations. Many research works have highlighted on the security of MANETs. Most of them deal with prevention and detection approaches to individual misbehaving nodes. In this regard The effectiveness of these approaches not that much strong when multiple malicious nodes collude together to generate a collaborative attack this may result to more 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 black hole and gray hole (known as variants of black hole attacks). In black hole attacks, 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 hostile 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 gray hole attacks, the hostile 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 gray hole/collaborative Black hole attacks using a dynamic source routing (DSR)-based routing technique. This DSR [4] involves two main processes:Route discovery and route maintenanceTo 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 efficiently detects the hostile nodes that attempt to launch gray hole /collaborative black hole attacks.In our scheme, the address of an adjacent node is used as bait destination address to bait hostile nodes to send a reply RREP message, and hostile nodes are detected using a reverse tracing technique. Any suspicious detected hostile node is kept in a black hole 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 previously mentioned goal.

II.EXISTING WORK:

Many research works have investigated the problem of hostile 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 black hole attacks. In addition, some of this method requires 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] 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 [7] 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 [8], which we considered as benchmark schemes for performance comparison purposes. In [9], 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.

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. This proposed detection scheme takes advantage of the characteristics of both the reactive and proactive schemes to design a DSR-based routing scheme able to detects gray hole/collaborative black hole attacks in MANETs.

III.PROPOSEDAPPROACH:

This paper proposes a detection scheme called the cooperative bait detection scheme (CBDS), which aims at detecting and preventing malicious nodes launching gray hole/collaborative black hole 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 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.

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. CBDS is DSR-based. As such, it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message. However, the source node may not necessary be able to identify which of the intermediate nodes has the routing information to the destination or which has the reply RREP message or the hostile node reply forged RREP. This scenario may result in having the source node sending its packets through the fake shortest path chosen by the malicious node, which may then lead to a black hole attack. To resolve this issue, the function of HELLO message is added to the CBDS to help each node in identifying which nodes are their adjacent nodes within one hop. This function assists in sending the bait address to entice the malicious nodes and to utilize the reverse tracing program of the CBDS to detect the exact addresses of malicious nodes. The baiting RREQ packets are similar to the original RREQ packets, except that their destination address is the bait address.

The CBDS scheme comprises three steps:

1) The initial bait step

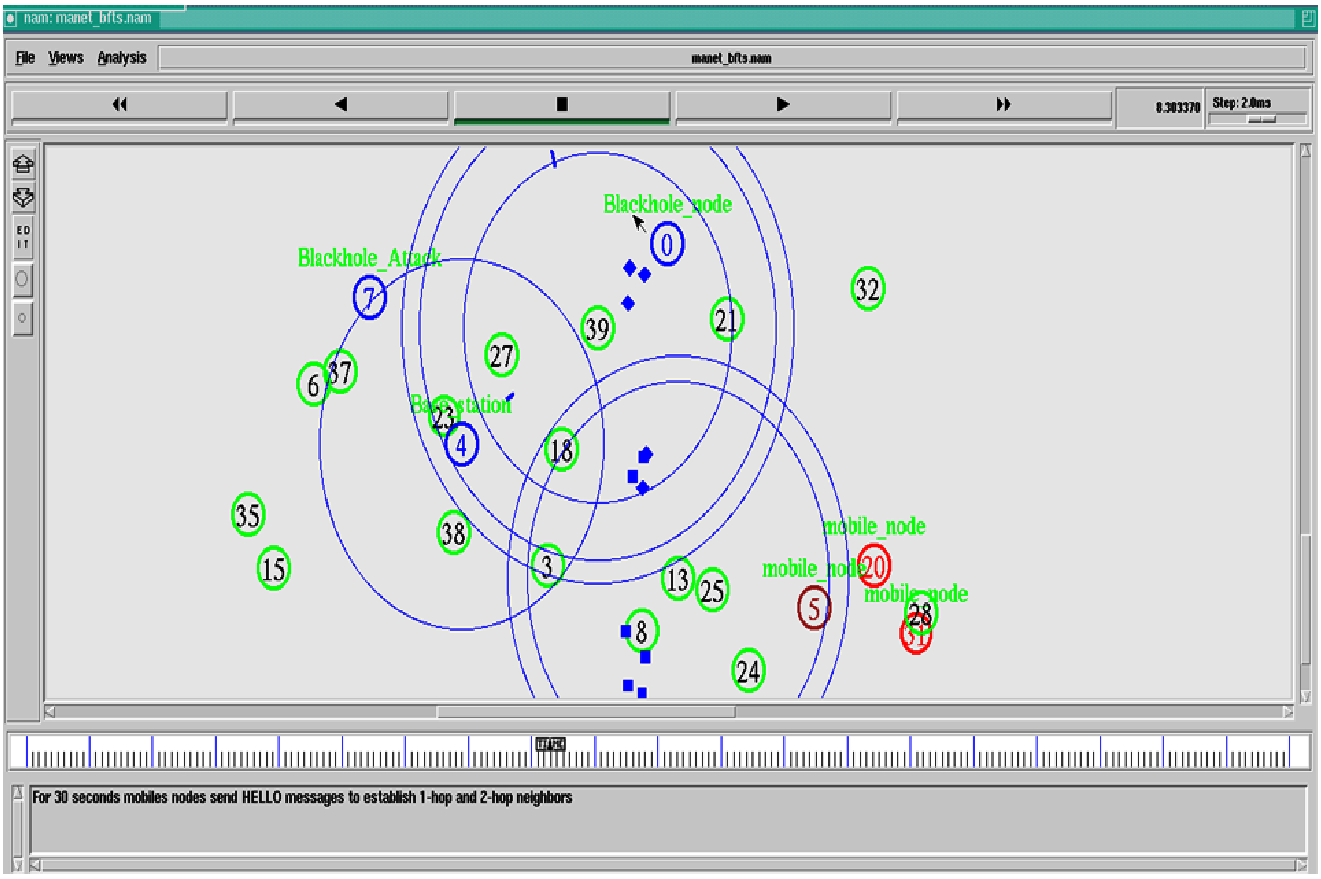
2) The initial reverse tracing step

3) The shifted to reactive defense step, i.e., the DSR route discovery starts process.The first two steps are initial proactive defense steps, whereas the third step is a reactive defense step.

IV.PERFORMANCE EVALUATION:

A.Simulation Parameter:

The ns 2.28[network simulator] 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 default threshold is set to 90%. All remaining simulation parameters are captured in Table III. The network used for our simulations is depicted in Fig. 5; and we randomly select the hostile nodes to perform attacks in the network.



For 30 seconds mobiles nodes send HELLO messages to establish 1-hop and 2-hop neighbors

Fig.5 Nam ouput of MANET with best effort fault tolerant (BEFT).

B.Performance Metrics:

We have compared the CBDS against the DSR [4],[9], and BFTR [13] schemes, chosen as benchmarks, on the basis of the following performance metrics.

1) 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 ith application, and pktsi is the number of packets sent by the source node in the ith application. The average packet delivery ratio of the application traffic n, which is denoted by PDR, is obtained as .

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

2) Routing Overhead:

This metric represents the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. Here, cpki is the number of control packets transmitted in the ith application traffic, and pkti is the number of data packets transmitted in the ith application traffic. The average routing overhead of the application traffic n, which is denoted by RO, is obtained as

$$RO = \frac{1}{n}\sum_{i=1}^{n}\frac{cpk_i}{pkt_i}.$$

3) Average End-to-End Delay:

This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is di, and the number of packets received by the destination node is pktdi. The average end-to-end delay of the application traffic n, which is denoted by E, is obtained as

$$E = \frac{1}{n}\sum_{i=1}^{n}\frac{d_i}{pktd_i}.$$

4) Throughput:

This is defined as the total amount of data (bi) that the destination receives them from the source divided by the time (ti) 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

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

TABLE III
SIMULATION PARAMETERS

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

Two simulation scenarios are considered:

1) Scenario 1: Varying the percentage of hostile nodes with a fixed mobility. MANET with best effort fault tolerant (BEFT).

2) Scenario 2: Varying the mobility of nodes under fixed percentage of hostile nodes. MANET with cooperative bait detection scheme and dynamic source routing (CBDS and DSR).

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

In Fig. 6, it can be observed that DSR drastically suffers from black hole attacks when the percentage of hostile nodes increases. This is attributed to the fact that DSR has no secure method for detecting/preventing black hole attacks.

Our CBDS scheme shows a higher packet delivery ratio compared with that of DSR. Even in the case where 40% of the total nodes in the network are hostile, the CBDS scheme still successfully detects those hostile nodes while keeping the packet delivery ratio above 90%. A threshold of 95% would then result in earlier route detection than when the threshold is 85% or is set to the dynamic threshold value. Thus, the packet delivery ratio when using a threshold of 95% is higher than that obtained when using a threshold of 85% or the dynamic threshold.

Second, we study the routing overhead of the CBDS and DSR for different thresholds. The results are captured in Fig. 7. In Fig. 7, it can be observed that when the number of malicious nodes increases, DSR produces the lowest routing overhead compared with the CBDS. This is attributed to the fact that DSR has no intrinsic security method or defensive mechanism.

In fact, the routing overhead produced by the CBDS for different thresholds is a little bit higher than that produced by DSR; this might be due to the fact that the CBDS would first send bait packets in its initial bait phase and then turn into a reactive defensive phase afterward. Consequently, a tradeoff should be made between routing overhead and packet delivery ratio. We have studied the effect of thresholds on the routing overhead.

As expected, it was found that the routing overhead of the CBDS reaches the highest value when the threshold is set to 95%. This is attributed to the fact that the detection scheme of CBDS triggers fast when the threshold value is 95% compared with when it is set to 85% or when it is equal to the dynamic threshold value. Thus, the bait packets will be sent many times in the network. It should be noticed that the dynamic threshold value can be adjusted according to the network performance.

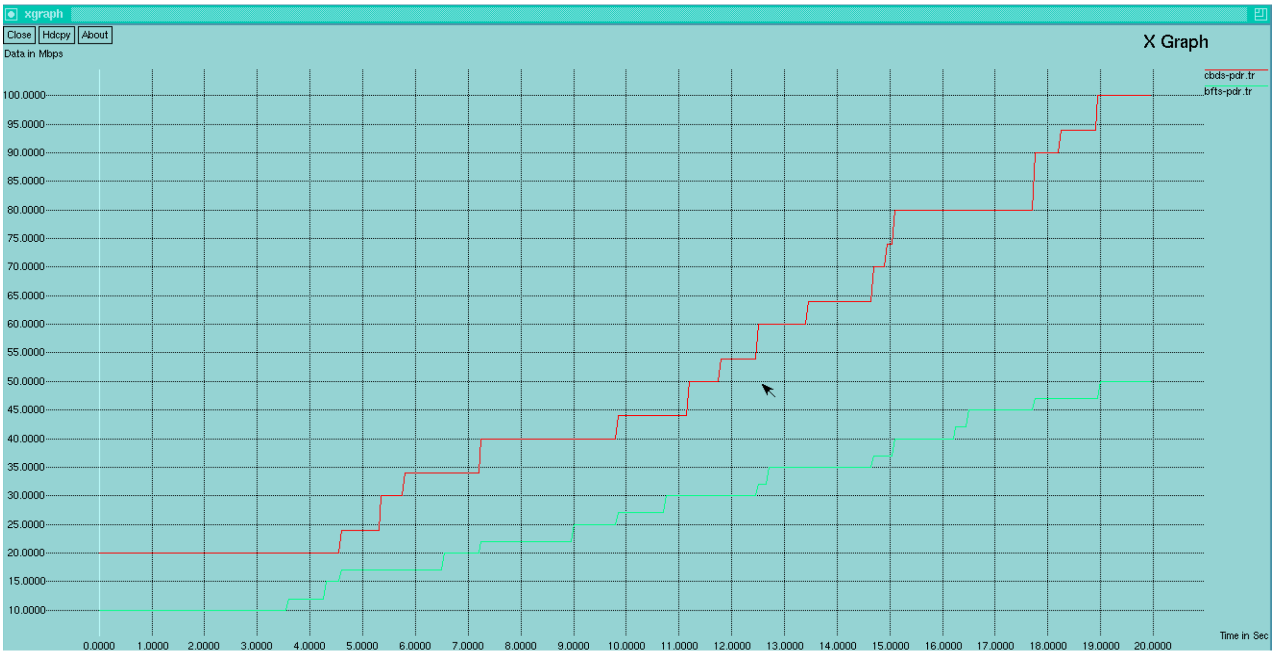


Fig.6 Packet delivery ratio of BEFT and the CBDS

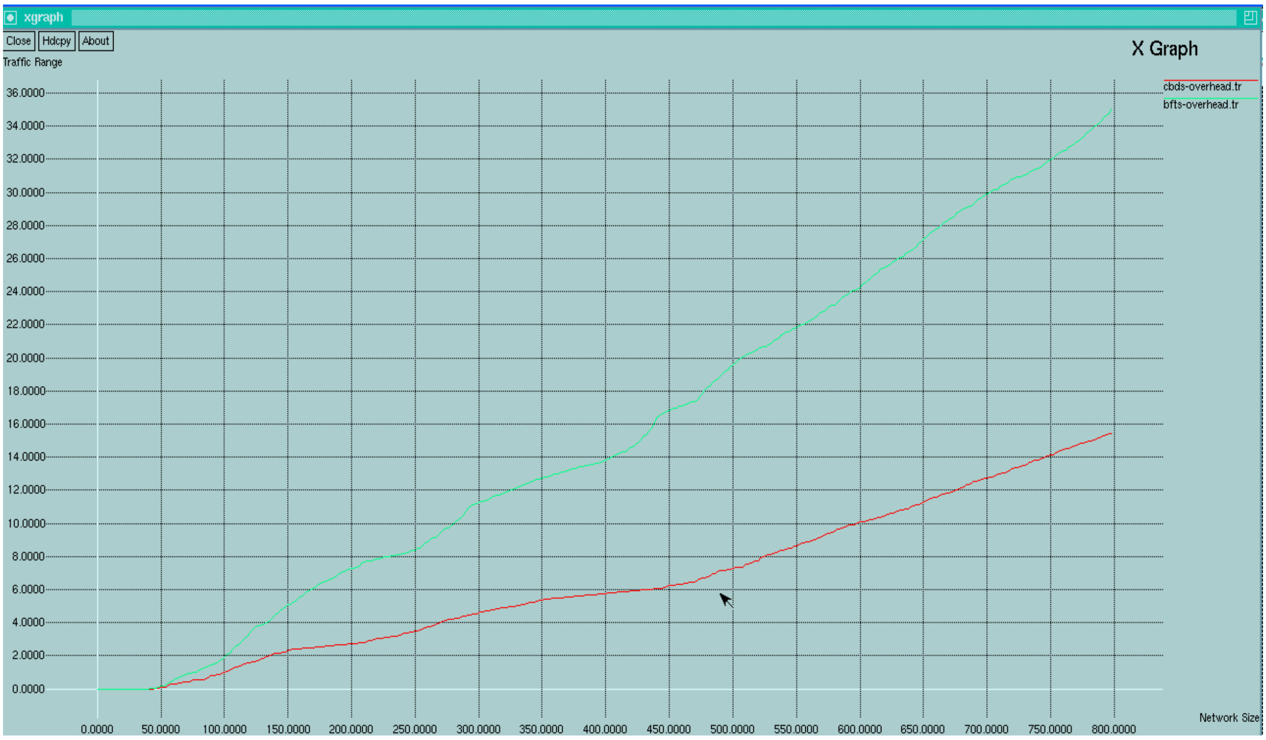


Fig.7 Routing overhead of BEFT and CBDS

V. CONCLUSION:

In document, we have proposed a new mechanism (called the CBDS) for detecting hostile nodes in MANETs under gray/collaborative black hole attacks. Our simulation results shows that the CBDS outperforms the DSR 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 to 2) 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 offender.

REFERENCES:

9*
[1] 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.

[2] C. Chang, Y.Wang, and H. Chao, "An efficient Mesh-based core multicastrouting protocol onMANETs," J. Internet Technol., vol. 8, no. 2, pp. 229–239, Apr. 2007.

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

[4] 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.

[5] 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.

[6] 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.

[7] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Compute., vol. 6, no. 5, pp. 536–550, May 2007.

[8] H. Deng, W. Li, and D. Agrawal, "Routing security in wireless ad hoc network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

[9] Y. Xue and K. Nahrstedt, "Providing fault-tolerant ad hoc routing service in adversarial environments," Wireless Pers.Commun., vol. 29, pp. 367–388, 2004.