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 6, June 2016

Prevention of Collaborative Attacks of Malicious Node in MANET Using CBDA Scheme

Deepali Tambekar, Prof. H. V. Kumbhar

P.G. Student, Department of Computer Engineering, Padmabhushan Vasantdada Patil Institute of Technology, University of Pune, India

Department of Computer Engineering, Padmabhushan Vasantdada Patil Institute of Technology, University of Pune, India

ABSTRACT: In mobile ad hoc networks (MANETs), an essential requirement for the foundation of communication among nodes is that nodes should coordinate with one another. In the presence of malicious nodes, this requirement may lead serious security concerns; for instance, such node may disturb the routing process. In this context, preventing or detecting malicious nodes launching grayhole or collaborative blackhole in challenge. This project attempts to determine this issue by designing a dynamic source routing (DSR)- based routing mechanism, which is referred to as the cooperative bait detection scheme(CBDS), that coordinates the advantages of both proactive and reactive defense architectures. Our CBDS system 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: Cooperative bait detection scheme (CBDS), collaborative bait detection, collaborative blackhole attacks, detection mechanism, dynamic source routing (DSR), grayhole attacks, malicious node, mobile ad hoc network (MANET).

I. Introduction

Due to the widespread availability of mobile devices, mobile ad hoc networks (MANETs), have been widely used for various important applications such as military crisis operations and emergency preparedness and response operations [1][2]. This is primarily due to their infrastructure less 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. 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. We have proposed a mechanism called "cooperative bait detection scheme" (CBDS) is presented that effectively detects the malicious nodes that attempt to launch gray hole /collaborative black hole attacks[4]. 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 mentioned goal. 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. 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.

II. Related work

1) Paper Name: Dynamic Source Routing in Ad Hoc Wireless Networks (1996). Author: David B. Johnson David A. Maltz Description:

An ad hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any established infrastructure or centralized administration. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. This paper presents a protocol for routing in ad hoc networks that uses dynamic source routing. The protocol adapts quickly to routing changes when host movement is frequent, yet requires little or no overhead during periods in which hosts move less frequently. Based on results from a packet-level simulation of mobile hosts operating in an ad hoc network, the protocol performs well over a variety of environmental conditions such as host density and movement rates. For all but the highest rates of host movement simulated, the overhead of the protocol is quite low, falling to just 1% of total data packets transmitted for moderate movement rates in a network of 24 mobile hosts. In all cases, the difference in length between the routes used and the optimal route lengths is negligible, and in most cases, route lengths are on average within a factor of 1.01 of optimal.

2) Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks (2010). Author: Abderrahmane Baadache, Ali Belmehdi. Description:

In wireless ad hoc networks, the absence of any control on packets forwarding, make these networks vulnerable by various deny of service attacks (DoS). A node, in wireless ad hoc network, counts always on intermediate nodes to send these packets to a given destination node. An intermediate node, which takes part in packets forwarding, may behave maliciously and drop packets which goes through it, instead of forwarding them to the following node. Such behavior is called black hole attack. In this paper, after having specified the black hole attack, a secure mechanism, which consists in checking the good forwarding of packets by an intermediate node, was proposed. The proposed solution avoids the black hole and the cooperative black hole attacks. Evaluation metrics were considered in simulation to show the effectiveness of the suggested solution.

3) Detection and Removal of Cooperative Black/Gray hole attack in Mobile ADHOC Networks (2009). Author: Vishnu K, Amos J Paul **Description:**

Mobile ad hoc networks (MANET) are widely used in places where there is little or no infrastructure. A number of people with mobile devices may connect together to form a large group. Later on they may split into smaller groups. This dynamically changing network topology of MANETs makes it vulnerable for a wide range of attack. In this paper we propose a complete protocol for detection & removal of networking Black/Gray Holes.

4) An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs (2007). Authors: Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan Description:

We study routing misbehavior in MANETs (Mobile Ad Hoc Networks) in this paper. In general, routing protocols for MANETs are designed based on the assumption that all participating nodes are fully cooperative. However, due to the open structure and scarcely available battery-based energy, node misbehaviors may exist. One such routing misbehavior is that some sel_sh nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. In this paper, we propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. Analytical and simulation results are presented to evaluate the performance of the proposed scheme.

5) Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks (2003). Author: Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard. Description:
Mobile ad hoc networks (MANETs) are extensively used in military and civilian applications. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. This generic characteristic of MANET has rendered it vulnerable to security attacks. In this paper, we address the problem of coordinated attack by multiple black holes acting in group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack.

III. PROPOSED SYSTEM

In this paper, a mechanism 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.

1. **Network Model.**
2. **Initial Bait.**
3. **Initial Reverse Tracing.**
4. **Shifted to Reactive Defense Phase.**
5. **Security Module**.

1. Network Model: It consider a dense multi hop static wireless mobile network deployed in the sensing field, it assume that each node has plenty of neighbors. When a node has packets to send to the destination, it launches the on-demand route discovery to find a route if there is not a recent route to a destination and the MAC layer provides the link quality estimation service.

2. 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 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 CBDA had initiated the DSR route discovery phase.

3. Initial 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 CBDA is able to detect more than one malicious node simultaneously when these nodes send reply RREPs.

4. Shifted to Reactive Defense Phase: When the route is established and if at the destination it is found that the packet delivery ratio 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 varying value in the range [85%, 95%] that can be adjusted according to the current network efficiency. The initial threshold value is set to 90%. A dynamic threshold algorithm is designed that controls the time when the packet delivery ratio falls under the same threshold. If the descending time is shortened, it means that the malicious nodes are still present in the network. In that case, the threshold should be adjusted upward. Otherwise, the threshold will be lowered.

5. Security Module: It is going to use the as key value of the message which is going to be sent and then it is added with the public key and sent from the source to destination through the intermediate node and then decrypted in the

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

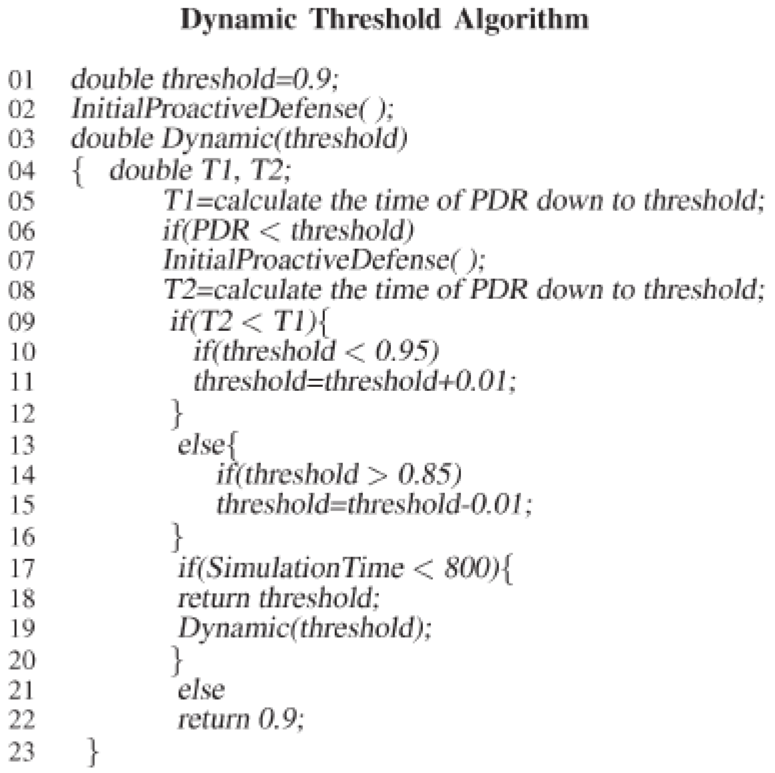
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

destination by subtracting the public key from the message obtained and then the original message is obtained from the packets sent.

IV. PSEUDO CODE

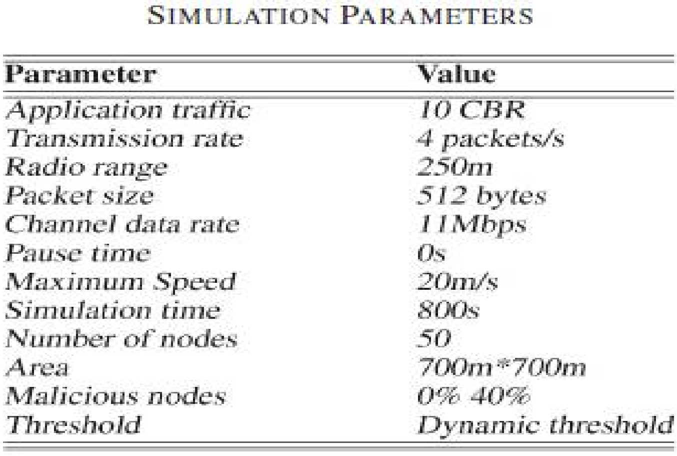


Dynamic Threshold Algorithm

```
double threshold=0.9;
InitialProactiveDefense( );
double Dynamic(threshold)
{   double T1, T2;
            T1=calculate the time of PDR down to threshold;
            if(PDR < threshold)
            InitialProactiveDefense( );
            T2=calculate the time of PDR down to threshold;
             if(T2 < T1){
                if(threshold < 0.95)
                threshold=threshold+0.01;
             }
             else{
                  if(threshold > 0.85)
                  threshold=threshold-0.01;
             }
             if(SimulationTime < 800){
             return threshold;
             Dynamic(threshold);
             }
             else
             return 0.9;
  }
```

V. SIMULATION RESULTS

We study the packet delivery ratio of the CBDS and DSR for different thresholds when the percentage of malicious nodes in the network varies from 0% to 40%. The maximum speed of nodes is set to 20m/s. The results are captured in Fig. 2. In Fig. 2, it can be observed that DSR drastically suffers from blackhole attacks when the percentage of malicious nodes increases. This is attributed to the fact that DSR has no secure method for detecting/preventing blackhole 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 malicious, the CBDS scheme still successfully detects those malicious nodes while keeping the packet delivery ratio above 90%.



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*

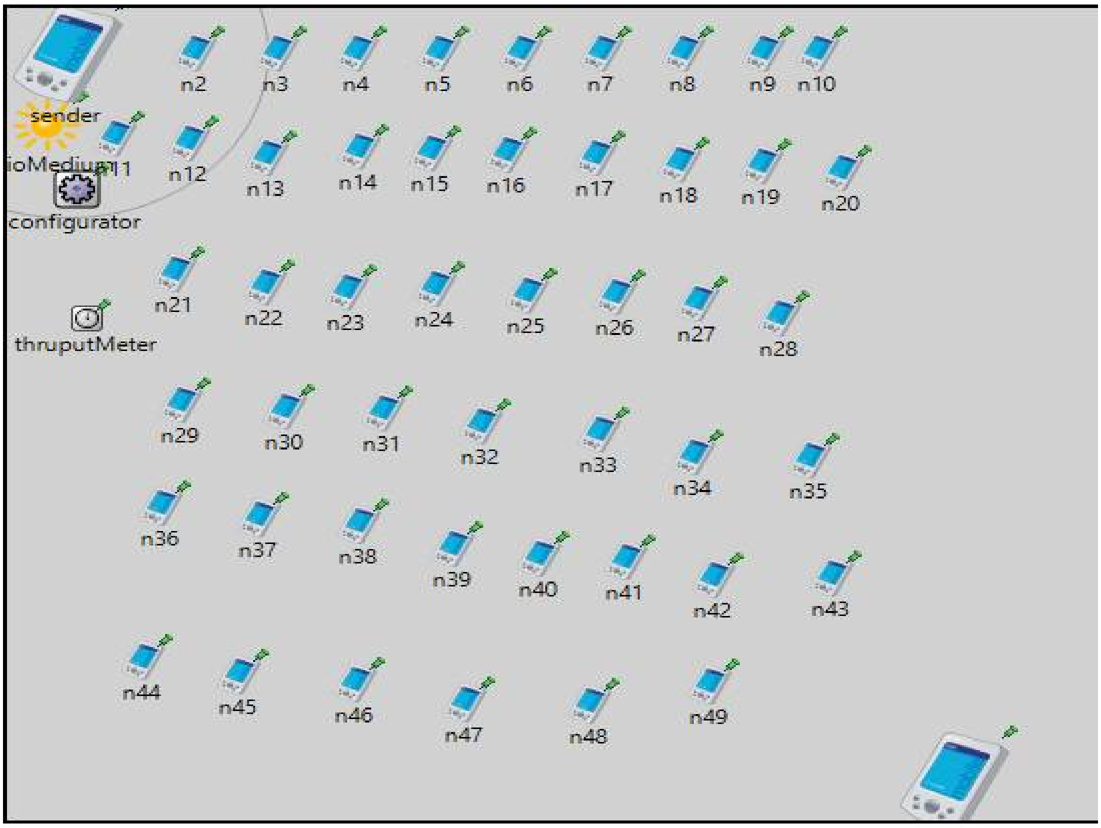


Figure 1 : Network of 50 nodes including sender and receiver

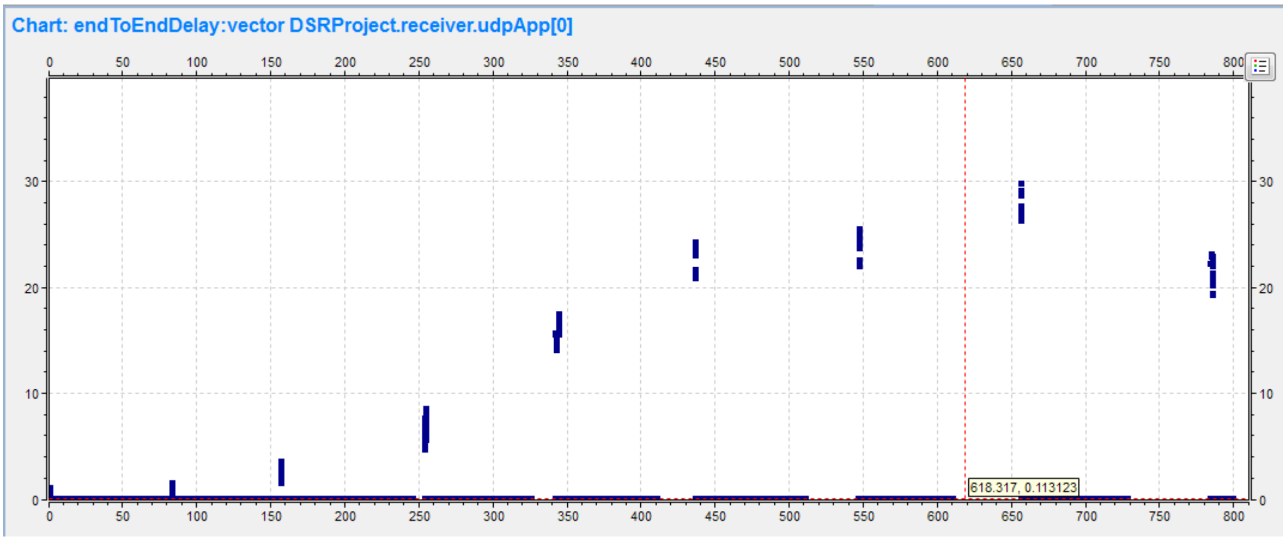


Figure 2 : End to end delay with respect to malicious node ratio and packet delivery ratio

VI. CONCLUSION AND FUTURE WORK

In this approach, we have proposed a new mechanism Cooperative Bait Detection Scheme (called the CBDS) for detecting malicious nodes in MANETs under gray/collaborative blackhole attacks. 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. We have observed that the CBDS outperforms the DSR, 2ACK, and BFTR schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio. 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. 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 miscreants.

REFERENCES

1. P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node forMANET based on hybrid defense architecture," in *Proc. 2nd Intl. Conf. Wireless Commun., VITAE*, Chenai, 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, Jan. 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 misbehavior 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.

BIOGRAPHY

Deepali R. Tambekar, Pursuing M.E in computer Engineering at Padmabhushan Vasantdada Patil Institute Of Technology, Pune.She received Bachelor of Engineering degree in 2007 from K.D.K.C.E., Nagpur MS, India