© 2016 IJEDR | Volume 4, Issue 3 | ISSN: 2321-9939

An approach for defending against collaborative attacks by malicious nodes in MANETs

[1]Miss Ashwini S. Barote , [2]Dr. P. M. Jawandhiya,

[1]PG Scholar, [2]Principal
[1]Computer Science and Engineering Department,
[1]PLITMS, Buldana, India

***Abstract*— 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. 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).**

***Index Terms*— MANET, CBDS, DSR, BFTR, RREP, RREQ**

I. INTRODUCTION

What is MANET?

The term MANET (Mobile Ad hoc Network) refers to a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self-organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Otherwise, a stand for “Mobile Ad Hoc Network” A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.

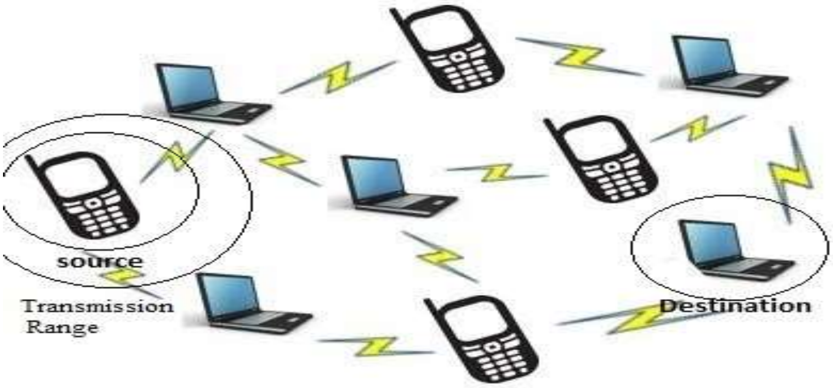


Fig 1.1 Structure of MANET

How MANET works?

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion and other factors. Approaches are intended to be relatively lightweight in nature, suitable for multiple hardware and wireless environments, and address scenarios where MANETs are deployed at the edges of an IP infrastructure. Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers) should also be supported by MANET specifications and management features.

Using mature components from previous work on experimental reactive and proactive protocols, the WG will develop two Standards track routing protocol specifications:

- Reactive MANET Protocol (RMP)

- Proactive MANET Protocol (PMP)

If significant commonality between RMRP and PMRP protocol modules is observed, the WG may decide to go with a converged approach. Both IPv4 and IPv6 will be supported. Routing security requirements and issues will also be addressed. The MANET WG will also develop a scoped forwarding protocol that can efficiently flood data packets to all participating MANET nodes. The primary purpose of this mechanism is a simplified best effort multicast forwarding function. The use of this protocol is intended to be applied ONLY within MANET routing areas and the WG effort will be limited to routing layer design issues. The MANET WG will pay attention to the OSPF-MANET protocol work within the OSPF WG.

II. LITERATURE REVIEW

2.1 CBDS: A Cooperative Bait Detection Scheme to prevent malicious node for MANET based on hybrid defense architecture

AUTHORS: P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen

With the widespread use of mobile devices, the users of Mobile Ad hoc network (MANET) become increasingly more, which results the rapid development of the technology. Due to MANET don't need the infrastructure, it can deploy fast and conveniently in any environment. Because of its easy deployment features, in addition to use in personal area networks, home area networks and so on. Specially, MANET suit for military operations and the emergent disasters rescue that need to overcome terrain and special purpose in urgent. However the dynamical network topology of MANET, infrastructure-less property and lack of certificate authority make the security problems of MANET need to pay more attention. The common routing protocols in current such as DSR AODV and so on almost take account in performance. They don't have the related mechanism about detection and response. Aiming at the possible attacks by malicious nodes, based on the DSR protocol, this paper presented a mechanism to detect malicious nodes launching black/gray hole attacks and cooperative black hole attacks, known as Cooperative Bait Detection Scheme (CBDS). It integrates the proactive and reactive defense architectures, and randomly cooperates with a stochastic adjacent node. By using the address of the adjacent node as the bait destination address, it baits malicious nodes to reply RREP and detects the malicious nodes by the proposed reverse tracing program and consequently prevents their attacks.

2.2 Dynamic source routing in ad hoc wireless networks

AUTHORS: D. Johnson and D. Maltz

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 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.

2.3 TBONE: A mobile-backbone protocol for ad hoc wireless networks

AUTHORS: I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero.

We introduce an ad hoe wireless mobile network that employs a hierarchical networking architecture. The network uses high capacity and low capacity nodes. We present a topological synthesis algorithm that selects a subset of high capacity nodes to form. a backbone network. The latter consists of interconnected backbone nodes that intercommunicate across high power links, and also makes use of (airborne, ground and underwater) Unmanned Vehicles (UVs). We introduce the TBONE protocol to implement the key networking schemes for such a Mobile Backbone Network (MBN). It includes combined network layer operation, i.e. mobile backbone net-work topological synthesis, and MAC layer resource allocation schemes. The TBONE protocol serves to allocate resources across the network to ensure that user applications are granted acceptable quality-of-service (QoS) performance, while striving to ensure a highly survivable and robust backbone-oriented networking architecture. We present elements of the protocol and key involved algorithms, and illustrate the distinctive advantages offered by the TBONE based mobile backbone network.

2.4 Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks

AUTHORS: A. Baadache and A. Belmehdi

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.

2.5 Mitigating routing misbehavior in mobile ad hoc networks

AUTHORS: S. Marti, T. J. Giuli, K. Lai, and M. Baker

This paper describes two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. We use a watchdog that identifies misbehaving nodes and a pathrater that helps routing protocols avoid these nodes.

Through simulation we evaluate watchdog and pathrater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increase throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility, watchdog and pathrater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24%.

2.6 Network Simulator

NS is an object oriented simulator, written in C++, with an OTcl interpreter as a frontend. NS uses two languages because simulator has two different kinds of things it needs to do. On one hand, detailed simulations of protocols require a systems programming language which can efficiently manipulate bytes, packet headers, and implement algorithms that run over large data sets. For these tasks run-time speed is important and turn-around time (run simulation, find bug, fix bug, recompile, re-run) is less important.

Network Simulator 2.33 (NS2)

Network Simulator (NS2) is a discrete event driven simulator developed at UC Berkeley. It is part of the VINT project. The goal of NS2 is to support networking research and education. It is suitable for designing new protocols, comparing different protocols and traffic evaluations. NS2 is developed as a collaborative environment. It is distributed freely and open source. A large amount of institutes and people in development and research use, maintain and develop NS2.

III. EXISTING SYSTEM

DSR 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.

3.1 Disadvantages Of Existing System

- 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 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.

IV. PROPOSED SYSTEM

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.

4.1 Advantages Of Proposed System

- 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.

V. REQUIREMENT ANALYSIS

5.1 Hardware Requirements

Processor	: Pentium –IV
Speed	: 1.1 GHz
RAM	: 256 MB(min)
Hard Disk	: 20 GB
Floppy Drive	: 1.44 MB
Key Board	: Standard Windows Keyboard
Mouse	: Two or Three Button Mouse
Monitor	: SVGA 4.2

5.2 Software Requirements

Operating System	:Fedora-8
Tool	:Network Simulator-2.32
Front End	:OTCL (Object Oriented Tool Command Language)
Back End	:C++

VI. SYSTEM DESIGN

6.1 Block diagram

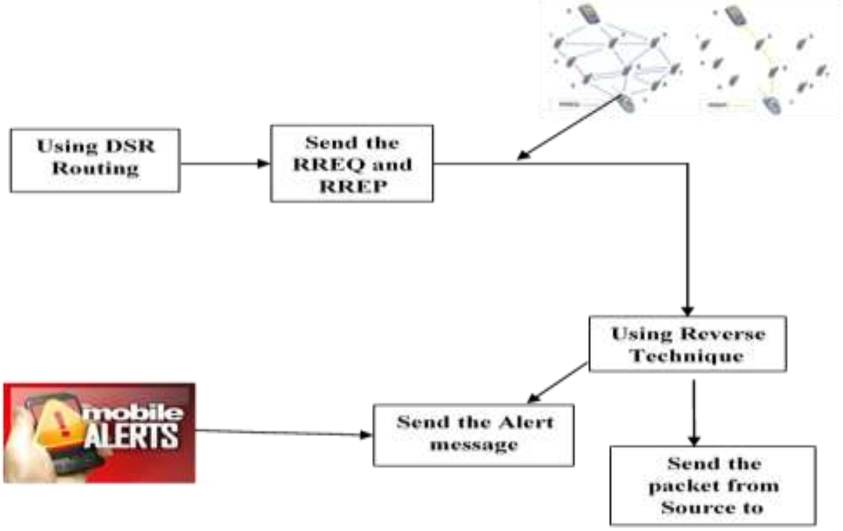


Fig. 6.1 Block Schematic Diagram

The DSR involves two main processes: route discovery and route maintenance. The source node broadcast the RREQ through the network. If an intermediate node has the route information to the destination node in its cache, it will reply with a RREP to the source node. When a RREQ is forwarded, the node adds its address information in the RREQ packet. When destination receives the RREQ, it can know all the information about intermediate node. Then the destination will reply with RREP to the source node along with the routing information.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.

VII. ALGORITHM

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 (T1 < T2) {
      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 ;
}
```

VIII. EXPERIMENTAL SETUP

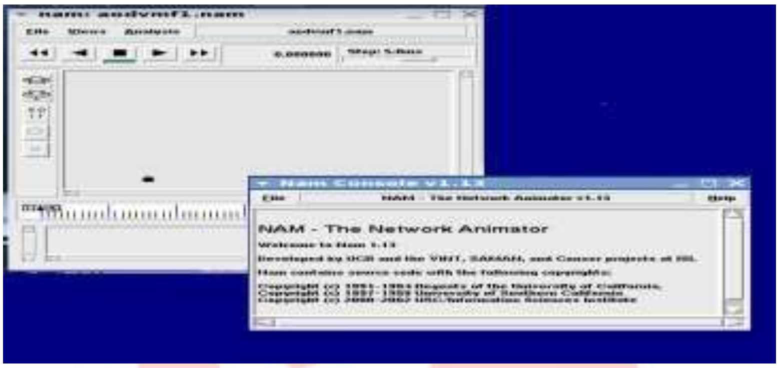
8.1 Fedora8 Terminal

Fedora8 terminal is used to run the TCL program. When we want to run NAM file or to show the result of TCL file give the path of file in terminal using cmd ns type the path of TCL file.

Fig.8.1 Snapshot of Terminal

8.2 Network Animator (NAM)

Nam is a Tcl/TK based animation tool for viewing network simulation traces and real world packet trace data. The design theory behind nam was to create an animator that is able to read large animation data sets and be extensible enough so that it could be used indifferent network visualization situations.



```
NAM - The Network Animator
Welcome to Nam 1.13
Developed by UCB and the VINT, SAMAN, and Conser projects at ISI.
Nam contains source code with the following copyrights:
Copyright (c) 1991-1994 Regents of the University of California.
Copyright (c) 1997-1999 University of Southern California
Copyright (c) 2000-2002 USC/Information Sciences Institute
```

Fig.8.2 Snapshot Of Network Animator (NAM)

IX. SIMULATION RESULTS

9.1System Snapshots

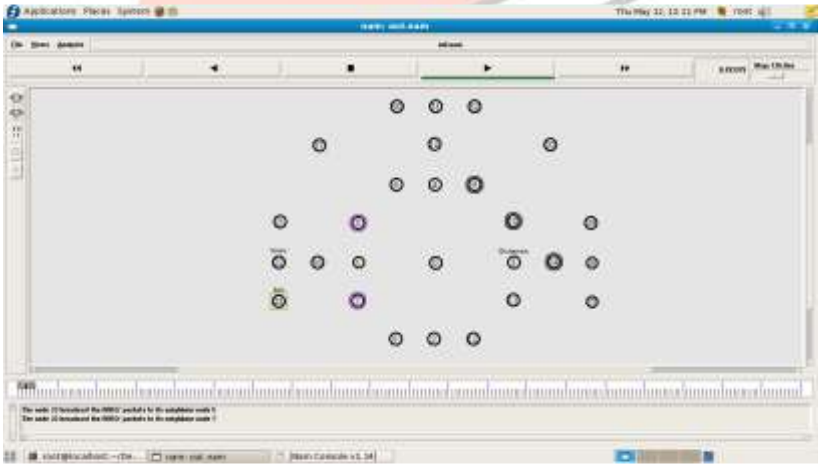


Fig 9. (a)Selecting adjacent node

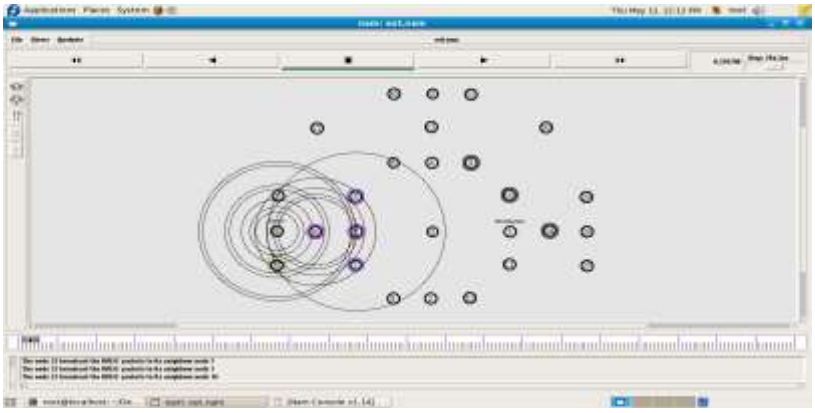


Fig 9. (b)Source node 22 broadcast request packets to its neighboring node

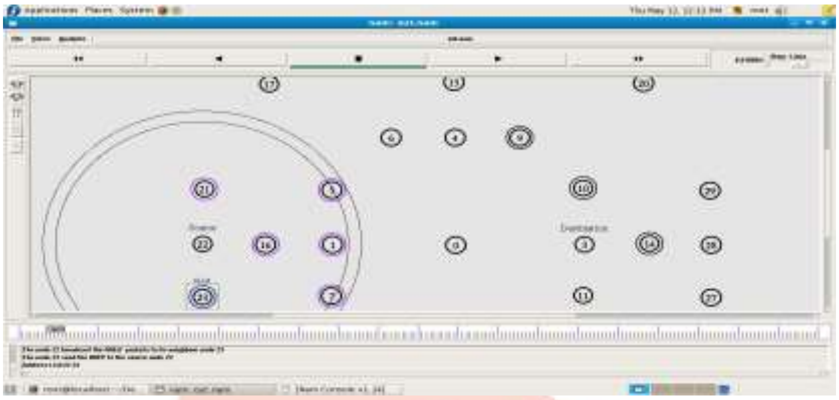


Fig 9. (c)Bait phase

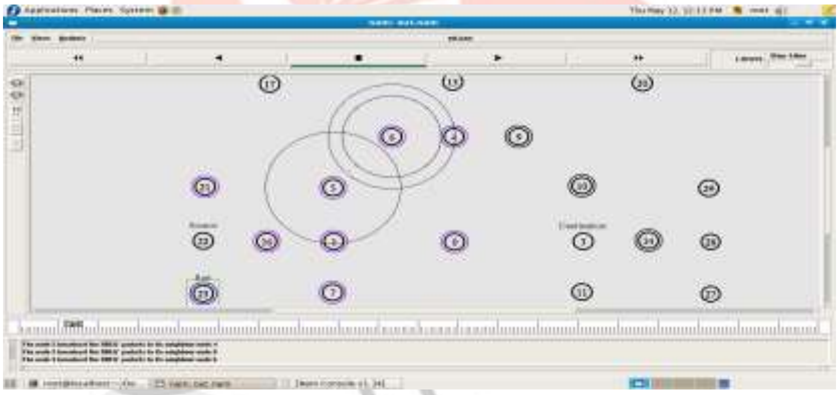


Fig 9. (d)Node 5 broadcast request packets to tits neighboring node

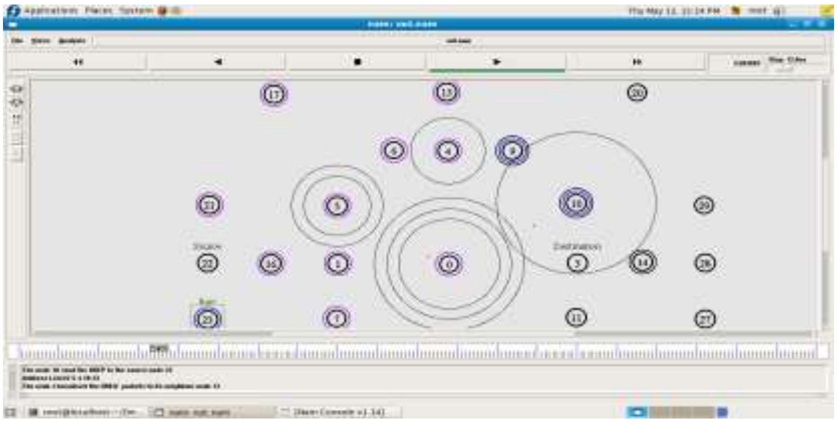


Fig. 9 (e) Node 10 send RREP packet to source node 22, including address list 22 5 4 10 23

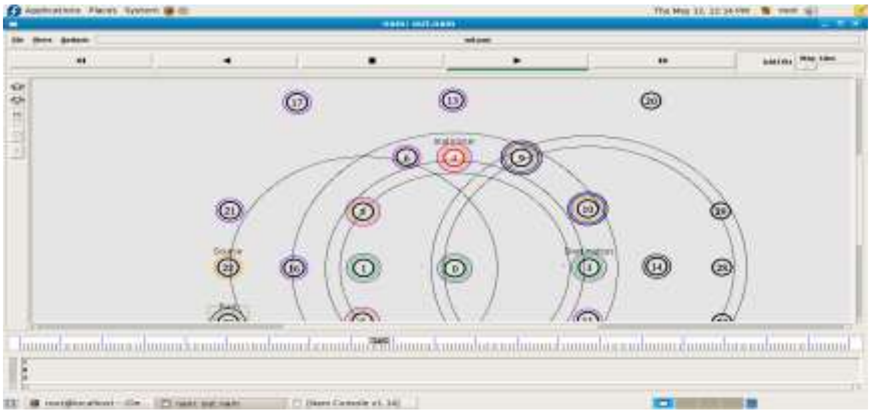


Fig. 9(f) Node 4 is detected as a malicious node

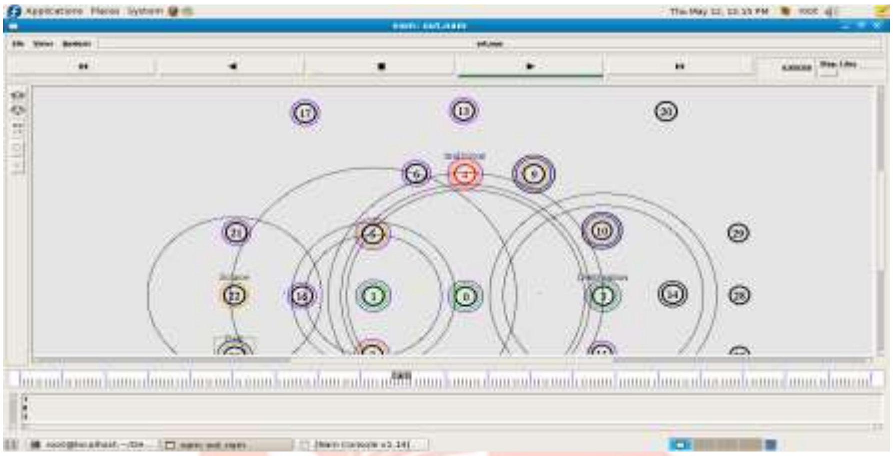


Fig.9 (g)Node 4 added to the blackhole list

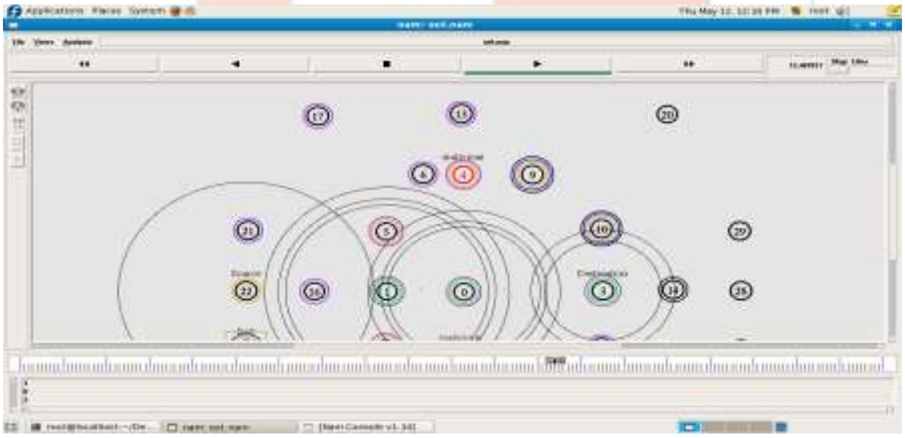


Fig.9 (h)Real shortest path to destination is 1-0-3

X. Graphical Representation

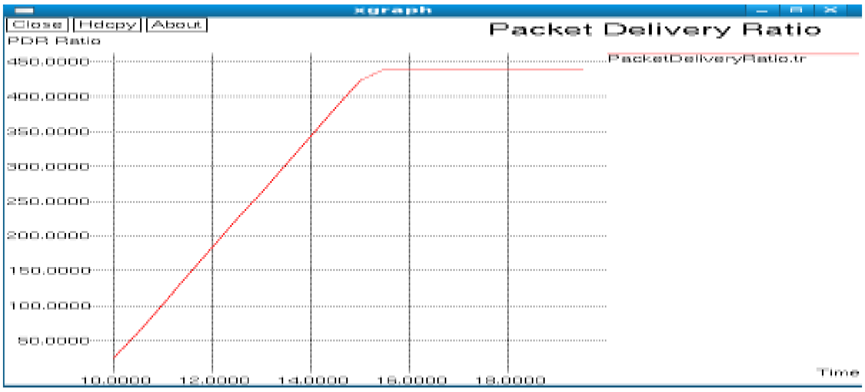


Fig. 10(a)Packet delivery ratio

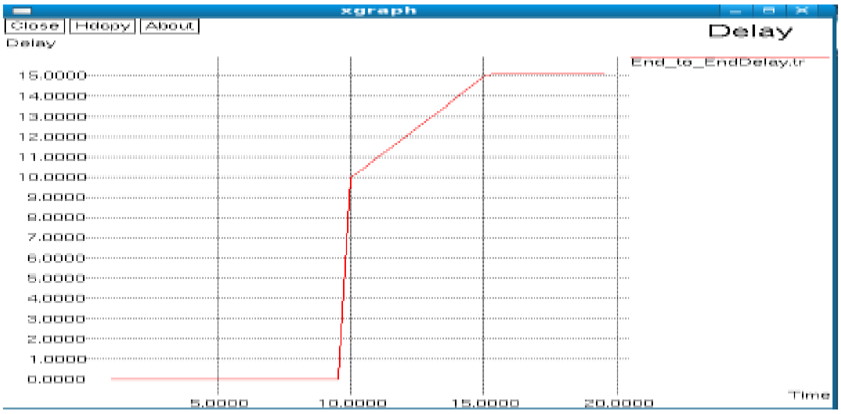


Fig. 10(b)End-to-End delay

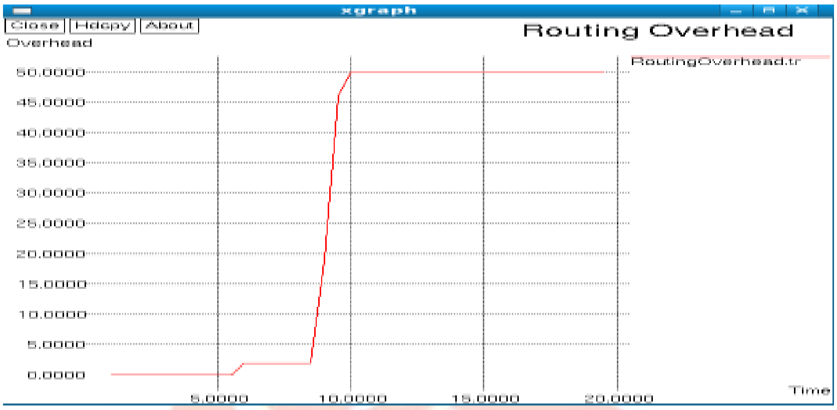


Fig. 10(c)Routing overhead

XI. CONCLUSION

In this project, 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 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] Vishnu K and Amos J Paul, “Detection and Removal of Cooperative Black/Gray Hole Attack in Mobile ADHOC Networks”, International Journal of Computer Applications, Vol. 1, No. 22, 2010.

[2] 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.

[3] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen, “CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture”, IEEE, 2011

[4] 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.

[5] 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.

[6] Sun B, Guan Y, Chen J, Pooch UW , “ Detecting Black-hole Attack in Mobile Ad Hoc Networks”. 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[7] Al-Shurman M, Yoo S-M, Park S , “ Black Hole Attack in Mobile Ad Hoc Networks”. 42nd Annual ACM Southeast Regional Conference (ACMSE’42), Huntsville, Alabama, 2-3 April 2004.

[8] Tamilselvan L, Sankaranarayanan V, “Prevention of Blackhole Attack in MANET”, 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 2730 August 2007.

[9] Djenouri D, Badache N, “Struggling Against Selfishness and Black Hole Attacks in MANETs”, Wireless Communications & Mobile Computing Vol. 8, Issue 6, pp 689-704, August 2008.

[10] Raj PN, Swadas PB, “DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET”, International Journal of Computer Science Issue, Vol. 2, pp 54–59, 2009.

[11] Himani Yadav, Rkesh Kumar, "A Review on Black Hole Attack in MANETs", International Journal of Engineering Research and Applications (IJERA) Vol.2 Issue 3, pp.1126-1131 Mayy-Jun 2012.
[12] Shahram Behzad, Shahram Jamali, Morteza Analoui, "A Survey over Black Hole Attack Detection in Mobile Ad Hoc Network", International Journal of Computer Science and Network Solutions, Vol 2.No.5 May.2014
[13] Nidhi Gupta, Sanjoy Das, Khushal Singh, "A Comprehensive Survey and Comparative Analysis of Black Hole Attack in mobile ad-hoc network", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol.8, no.1, 2014.
[14] Chandni Garg, Preeti Sharma, Prashant Rewagade ,"A Literature Survey of Black Hole Attack on AODV Routing Protocol", International Journal of Advancement in Electrical and Computer Engineering (IJAECE) Vol 1, Issue 6, pp.152.157 Sep 2012.

Authors:

Miss. Ashwini S. Barote Student of Second year M.E. (Computer Science and Engineering) Pankaj Laddhad Institute of Technology and Management Studies, Buldana Sant Gadge Baba Amravati University. Has earned degree of B.E (Computer Science and Engineering) from Sant Gadge Baba Amravati University in 2014.

Dr. P. M. Jawandhiya, Principal, (Computer Science and Engineering) Pankaj Laddhad Institute of Technology and Management Studies, Buldana Sant Gadge Baba Amravati University. Has earned degree of B.E (Computer Engineering), M.E. (Computer Sci. & Engg.), Ph.D. in Engg. & Tech. (Computer Sci. & Engg.), M.B.A. (Human Resource & Management)