Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 1, Number 2; November, 2014 pp. 30-34

http://www.krishisanskriti.org/acsit.html

Defending Against Byzantine and Resource Consumption Attacks by Malicious Nodes in MANETs

Neha Mahajan[1], Rajeev Bedi[2] and S.K Gupta[3]

[1,2,3]Department of Computer Science Beant College of Engineering and Technology, Gurdaspur, Punjab
E-mail: [1]nehacu29@gmail.com, [2]rajeevbedi@rediffmail.com, [3]skgbcetgsp@gmail.com

Abstract: *A mobile ad hoc network (MANET) is a wireless network that does not depend on any fixed structure (i.e., routing facilities, such as wired networks and access points), and whose mobile nodes must cooperate among themselves to regulate connectivity and routing. Attacks where adversaries have full control of a number of authenticated devices and behave randomly to disrupt the network are stated as Byzantine attacks. While in resource consumption attack, an attacker tries to consume or waste away resources such as bandwidth, computational power, and battery power of other nodes present in the network. In this context, preventing or detecting malicious nodes launching byzantine and resource consumption attacks is of mere concern. The objective of this paper is to utilize a hybrid mechanism, referred to as Cooperative Bait Detection Scheme, which is based on DSR routing protocol to detect the byzantine and resource consumption attacks.*

Keywords*:* *malicious attacks, byzantine attack, resource consumption attack, CBDS*

1. INTRODUCTION

In this paper, a mechanism called cooperative bait detec- tion scheme (CBDS), is utilized to effectively detect the malicious nodes that attempt to launch byzantine and resource consumption attacks. This scheme is implemented in two steps i.e., the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and then in second step, malicious nodes are detected using a reverse tracing technique. [6]

Byzantine attack is the most likely attack in which the set of the compromised nodes are able to take part in communication while behaving like a normal nodes and make a communication robust but with a forged packet delivery associated with it. The detection of such attacks is very difficult as well as time consuming [17]. In Resource consumption attack the malicious node or attacker tries to consume both the network and node resources by generating and sending frequent unnecessary routing traffic. This routing traffic can only be RREQ and RERR packets. The aim of this attack is to flood the network with false routing packets to consume all the available network bandwidth with irrelevant traffic and to consume energy and processing power from the nodes. [4]

The main focus in this paper is on detecting byzantine and resource consumption attacks using a dynamic source routing–(DSR) based routing scheme. DSR [6] mainly includes two main routes: route discovery and route maintenance. For execution of the route discovery phase, the source node broadcasts a Route Request (RREQ) packet through the MANET. 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. If an intermediate node has routing information to the destination in its route cache, it will reply with a RREP to the source node. 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 entire routing information of the recognized route. DSR does not have any type of detection mechanism, but the source node can get all route information concerning the nodes on the route. In CBDS approach, the scheme would be able to detect such nodes and will not communicate further with that node.

2. GENERAL APPROACH

In CBDS approach the source node stochastically selects an adjacent node with which to cooperate, in the logic that the address of this node will be used as bait destination address to bait malicious nodes to send a reply RREP message. Further, using a reverse tracing technique malicious nodes are thereby distinguished and prevented from participating in the routing operation. It is expected that when there will be a significant drop 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 CBDS scheme merges the advantage of both proactive and reactive detection schemes response respectively in instruction to decrease the resource wastage.[6]

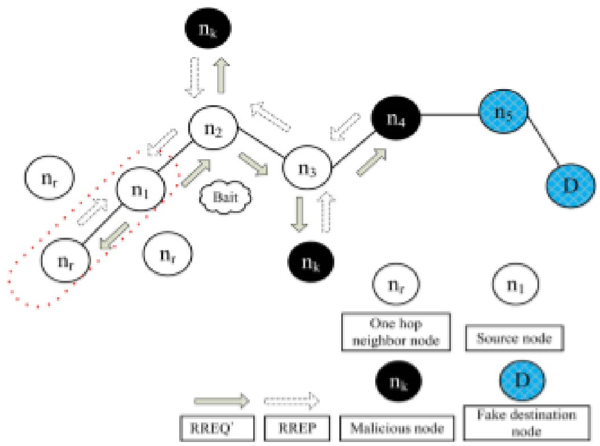


Fig. 1: Random Selection of a cooperative bait address

This CBDS scheme mainly includes two phases:

Executing both the phases, we will be able to defend the network from byzantine attack and hence the performance of the network will increase.

Phase I-The objective of this phase is to entice a malevolent node to send a route reply RREP by sending the bait RREQ' that it has used to advertise itself as having the shortest path to the node.. To achieve this objective, the algorithm in the Algorithm1 has been designed to generate the destination address of the bait RREQ'. The source node randomly selects an adjacent node, i.e., n_r, within its one-hop neighborhood nodes and collaborates with this node by taking its address as the destination address of the bait RREQ'. Because each node baits randomly, the adjacent node would be changed if the node moved; the bait would not remain unchanged. There is some follow-up phase I analysis as follows: Firstly, if the n_r node had not launched an attack, then after the source node had sent out the RREQ', there would be other nodes' reply RREP in addition to that of the n_r node. This specifies that the malicious node existed in the reply routing, as shown in Fig. 1. [6] Therefore, a reverse tracing program in the next phase would be started in order to detect this route. If only the n_r node had sent the reply RREP, it means that there was no other malicious node present in the network and that the CBDS had originated the DSR route discovery phase.

Furthermore, if n_r was the malicious node of the attack, then after the source node had sent the RREQ', other nodes would have also sent reply RREPs. This would indicate that malicious nodes existed in the reply route. In this case, the reverse tracing program in the next phase would be initiated to detect this route. If n_r intentionally gave no reply RREP, it would be directly listed on the attack list by the source node. If only the n_r node had sent a reply RREP, it would mean that there was no other malicious node in the network, except the route that n_r had provided; in this case, the route discovery phase of DSR will be started. [6]

Algorithm 1

Input: N number of nodes, Source Node S, Destination Node D

Output: Malicious node detection

For each node n_i

Repeat

Phase 1

Select adjacent node n_r randomly from *S*

Location of selected node is taken as *D*

Send the RREQ' to the path

The RREP of other nodes on path to n_r is received

If reply $RREP \in n_r$

No other malicious node detected

Else

Presence of malicious attack

Phase 2

If n_m reply to false RREP

Record the address list in RREP

If n_k receives RREP

Separate the address list from *S* to *D*

K_k finds the route information to *D*

For K_k to be non-malicious

(a) Compare each node n_k to IP of RREP

(b) Find the next hop of n_k

(c) Select a hop of n_k

If *(a)* $\neq$ *(b) and (c)*

K_k can perform forward back

$Z=K1 \cap K2 \cap \ldots\ldots \cap Kn$ Dubious path

The reverse tracing operation in phase II will be directed for nodes receiving the RREP, with the goal to deduce the dubious path information. It should be highlighted that the CBDS is able to detect more than one malicious node simultaneously when these nodes send reply RREPs. Indeed, when a malicious node (initiating byzantine attack), for example, n_m, replies with a false RREP, an address list $P=\{n1,\ldots n_k,\ldots n_m,\ldots n_r\}$ is recorded in the RREP. If node n_k receives the RREP, it will separate the P list by the destination address n1 of the RREP in the IP field and get the address list $K_k=\{n1,\ldots n_k\}$, where K_k represents the route information from source node n1 to destination node n_k. Then, node nk will determine the differences between the address list $P=\{n1,\ldots n_k,\ldots n_m,\ldots n_r\}$ recorded in the RREP and $K_k=\{n1,\ldots n_k\}$. Therefore, we get

$$K_k' = P - K_k = \{nk+1,\ldots n_m,\ldots n_r\} \quad (1)$$

Where $K_{k'}$ represents the route information to the destination node (recorded after node nk).

To avoid interference by malicious nodes and to ensure that $K_{k'}$ does not come from malicious nodes, if node n_k received the RREP, it will compare:

a) Compare the source address in the IP fields of the RREP;

b) Find the next hop of n_k in the P={n1,... n_k,...nm, ...nr};

c) Select a one hop of n_k.

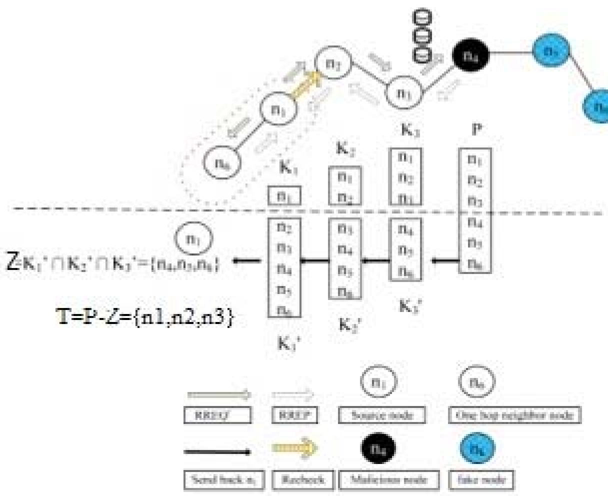


Fig. 2: Phase II of CBDS

If (a) is not the same with (b) and (c), then the received $K_{k'}$ can perform a forward back. Otherwise, n_k should just forward back the $K_{k'}$. In Fig. 3, although n4 can reply with K4'={n5, n6}, n3 will check and then remove K4' when it receives the RREP. After the source node obtains the intersection set of $K_{k'}$, the dubious path information S replied by malicious nodes could be detected, i.e.

$$Z=K1' \cap K2' \cap K3' ... \cap K_{k'}. \quad (2)$$

A malevolent node would reply the RREP to every RREQ, nodes that are present in a route before this action happened are assumed to be trusted. The set difference operation of P and Z is conducted to acquire a temporarily trusted set T, i.e.

$$T=P-Z. \quad (3)$$

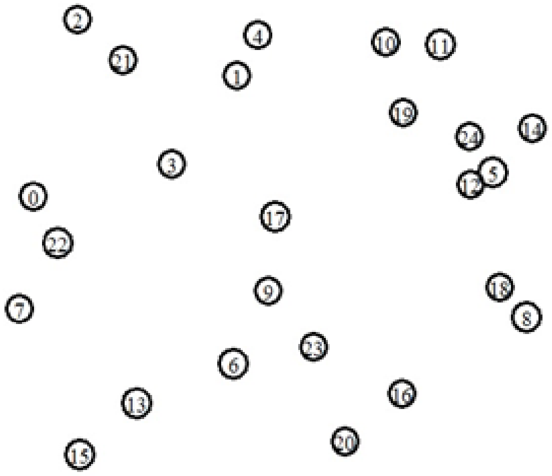
For the confirmation, that the malicious node (initiating byzantine attack) is in set Z, the source node would send the test packets to this route and would send the recheck message to the second node toward the last node in T. The source node will then store the node in an attack list and broadcast the alarm packets through whole network to update all other nodes to dismiss their operation with this node.

If the last node drops the packets instead of diverting them, the source node would store it in the attacks list. The states faced by malicious nodes in the route are illustrated in Fig. 2. Here, only a single malicious node n4 exist in the route, the source node n1 make up to send a packet to node n6. Node n4 replies with a false RREP along with the address list P={n1,n2,n3,n4,n5,n6}, only after n1 sends the RREQ' node. Here, node n5 and n6 are random nodes filled in by n4. If n3 had receive the replied. RREP by n4, it would separate the P list by the destination address n1 of the RREP in the IP field and get the address list K3={n1,n2,n3}. It would then conduct the set difference operation between the address lists P and K3={n1,n2,n3} to acquire K3'=P−K3={n4,n5,n6}, and would reply with the K3' and RREP to the source node n1 according to the routing information in P. Similarly, n2 and n1 would also perform the same operation after receiving the RREP; and will obtain K2'={n3,n4,n5,n6} and K1'={n2,n3,n4,n5,n6}, respectively; and then will send them back to the source node for intersection. The uncertain path information of the malicious node, i.e., Z=K1' ∩ K2' ∩ K3'={n4, n5, n6}, is obtained. The source node then calculates P − Z=T={n1, n2, n3} to acquire a temporarily trusted set. At the end, the source node will send the test packets to this path and the recheck message to n2, requesting it to enter the immoral mode and listening to n3. It could be found that n3 might divert the packets to the malicious node n4; hence, n2 would return the listening result to the source node n1, which would record n4 in an attack list, as the result of the listening phase. In Fig. 2, there was a single malicious node n4 in the route, which responded with a false RREP and the address list P={n1, n2, n3, n5, n4, n6}, then this node would have purposely selected a false node n5 in the RREP address list to interfere with the follow-up operation of the source node. However, the source node would have to intersect the received Kk' to obtain Z=K1'∩K2'∩K3'={n5, n4, n6} and T=P −Z={n1, n2, n3} and request n2 to listen to the node that n3 might send the packets to. As the result of this listening phase, the packets that should have been diverted to n5 by n3 should have been sent to n4. The source node would then store this node to the attacks list. In Fig. 3, if n5 and n4 were cooperative malicious nodes, we would obtain T=P-Z={n1, n2, n3} and n2 would be requested to listen to which node n3 might send the packets. Either n5 or n4 would be detected, and their cooperation stopped. Hence, the remaining nodes would be baited and detected. Fig. 2 illustrates that even if there were more malicious nodes in MANETs, the CBDS would still detect them simultaneously when they send the reply RREP.

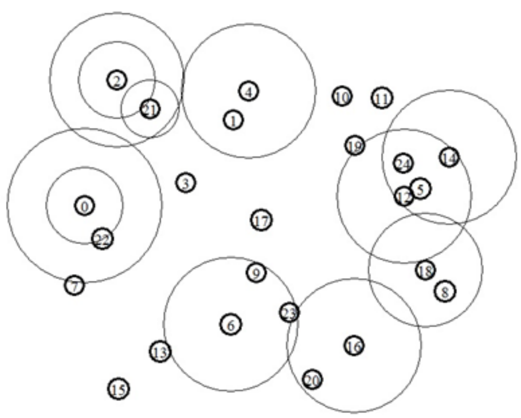
3. SIMULATION SCREENSHOTS

There are some screenshots presented below after the execution of the above algorithm. The execution of the same has been done on 25 nodes in the network with assistance of windows platform through Cygwin Terminal and NS2 Simulator.

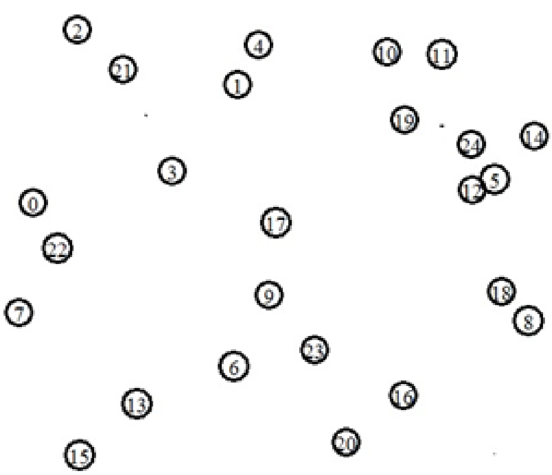
1) Network Initialization



2) Packet Broadcasting and Reply



3) Finding Malicious Nodes Path



In the Byzantine attack the attacker creates nodes, routing loops and forwards packets through non-optimal path or selectively dropping packets degrading the routing services as detailed in the algorithmic explanation above.

Whereas in resource consumption attack the attacker consumes the resources like bandwidth, computational power, and battery power of other nodes in the network. Since the attacker in CBDS approach will defend the attacker to participate further in networking, this will help to reduce packet loss and ultimately improve network performance and increases packet delivery ratio.

The increase in the performance of the network using CBDS can be viewed as graphs in the next paper based on analysis of some existing techniques. A comparative analysis will be presented using parameters Packet Delivery Ratio, End-to-End Delay, throughput and routing overhead.

4. CONCLUSION & FUTURE WORK

The CBDS approach is a hybrid approach that comprises of proactive and reactive architecture. We have used this approach for defending the network from byzantine and resource consumption attacks. As a future work, we intend to evaluate the performance of the network based on the Qos parameters such as packet delivery ratio, throughput, end-to-end delay and routing overhead. Also the comparative analysis would be done with the existing techniques based on the above mentioned parameters. Performance evaluation will let us know that there is very less consumption of resources using CBDS approach since the packet delivery ratio will be more using the above algorithm.

REFERENCES

[1] Abhay Kumar Rai, Rajiv RanjanTewari and Saurabh Kant Upadhyay(2010), Different Types of Attacks on Integrated MANET-Internet Communication, International Journal of Computer Science and Security (IJCSS) Volume 4: Issue 3

[2] AdityaBakshi, A.K.Sharma and Atul Mishra(2013), Significance of Mobile AD-HOC Networks (MANETS), International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-2, Issue-4

[3] DevuManikantanShila, Student Member, IEEE, Yu Cheng, Senior Member, IEEE, and Tricha Anjali, Senior Member, IEEE (2010), Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMN, IEEE Transactions on wireless communications, Vol. 9, No. 5

[4] Dilip Vishwakarma, Deepak Chopra(2012), An Efficient Attack Detection System for Mobile Ad-hoc Network, International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249–8958, Volume-1, Issue-6

[5] G. S. Mamatha and Dr. S. C. Sharma (2010), A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS, International Journal of Computer Science and Security, Volume 4: Issue 3

[6] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai (2014), Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait DetectionApproach, Systems Journal, IEEE ,Volume: PP, Issue: 99 , January 2014.

[7] MahaAbdelhaq, RaedAlsaqour, Mohammed Al-Hubaishi, Tariq Alahdal, and MueenUddin (2013), The Impact of Resource Consumption Attack on Mobile Ad- hoc Network Routing, International Journal of Network Security

[8] Maha Abdelhaq, Rosilah Hassan, Mahamod Ismail and Daud Israf, “Detecting Resource Consumption Attack over MANET using an Artificial Immune Algorithm”, Research Journal of Applied Sciences, Engineering and Technology 3(9): 1026-1033, 2011 ISSN: 2040-7467 © Maxwell Scientific Organization, 2011

[9] PradeepRai and Shubha Singh (2010), A Review of ‘MANET’s Security Aspects and Challenges’, IJCA International Journal of Computer Applications Special Issue on “Mobile Ad-hoc Networks” MANETs

[10] ReenaSahoo and D.r P.M Khilar (2011), Detecting Malicious Nodes in MANET based on a Cooperative Approach, International Journal of Computer Applications

[11] Seyed Mohammad AsghariPari, Mohammad Noormohammadpour, Mohammad JavadSalehi (2013), A Self-Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks approach, Wireless Days (WD), 2013 IFIP,IEEE

[12] ShabirSofi, Eshan Malik, Rayees Baba, Hilal Baba and Roohie Mir (2012), Analysis of Byzantine Attacks in Adhoc Networks and Their Mitigation, Communication and Information technology (ICCIT)

[13] Weichao Wang, Bharat Bhargava and Mark Linderman (2009), Defending against Collaborative Packet Drop Attacks on MANETs, 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS)

[14] Wenjia Li and Anupam Joshi (2011), Security Issues in Mobile Ad Hoc Networks-A Survey, International Journal of computer applications

[15] Yanwei Wang, F. Richard Yu, Senior Member, IEEE, Helen Tang, Senior Member, IEEE, and Minyi Huang, Member, IEEE (2014), A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks, Wireless Communication, IEEE Transactions on (Volume: 13, Issue-3)

[16] Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei(2006), A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks, Wireless/Mobile Network Security,Springer

[17] Apeksha. .B.Dhakde, Sonali.U.Nimbhorkar, Distributed Detection Methods for Byzantine Attack in Tree Topology, International Journal of Computer Applications (0975–8887) Volume 90–No 18, March 2014