ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

SECURITY FOR MOBILE ADHOC NETWORK AGAINST MALICIOUS NODES USING ADVANCED COOPERATIVE BAIT DETECTION SCHEMA (ACBDS)

M.Harini[1], *PG Scholar, Department of CSE, Kongu Engineering College, Tamilnadu*

Dr.K.Sangeetha[2] , *Assistant Professor(SRG), Department of CSE, Kongu Engineering College ,Tamilnadu*

ABSTRACT

Wireless networks are computer networks that are not connected by cables of any kind. The utilization of wireless network allows enterprises to avoid the costly process of introducing cables into buildings or as a connection association between completely different equipment locations. Wireless networks are at risk of completely different variety of attacks. MANET is the mobile wireless network that operates independently without any special hardware needs.

A detection scheme called the Advanced cooperative bait detection scheme (ACBDS) is proposed that aims at detecting and preventing malicious nodes by launching rushing and black hole attacks to collaborate in MANETs environment. To resolve this issue AODV protocol is used enhancing the performance of the MANETs environment. Proposed system helps in defending against the black hole attack and rushing attacks without any special hardware requirements.

Keywords- *Malicious, Rushing Attack, Blackhole Attack, Collaborative Detection*

I.INTRODUCTION

A mobile adhoc network (MANET) may be a self-configuring network of mobile routers and associated hosts connected via wireless links. These routers are free to move and organize themselves in a random manner. Thus, this wireless topology may change rapidly and unpredictably. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology. Minimal configuration and quick deployment make adhoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc.

Black Hole Attack

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will invariably have the provision in replying to the route request and so intercept the data packet and retain it. In protocol

based on flooding, the malicious node reply will be received by the requesting node before the reception of reply from actual node; hence a malicious and forged route is created. When this route is establish, now it's up to the node whether or not to drop all the packets or forward it to the unknown address. The method however malicious node fits within the data routes varies.

Rushing attack

In this type of attack, an adversary node which receives a Route Request packet from the source node floods the packet quickly throughout the network before other nodes that conjointly receive the same Route Request packet will react. Nodes that receive the legitimate Route Request packets assume those packets to be duplicates of the packet already received through the adversary node and hence discard those packets. Any route discovered by the source node would contain the adversary node as one of the intermediate nodes. Hence, the source node would not be ready to realize find secure routes. It is extremely tough to observe such attacks in MANET.

II.RELATED WORK

The detailed background study done related to this project is presented in the following section.

Tsou et al. (2011) presented a mechanism to find 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 random 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.

Deng et al. (2002) proposed a solution for the black hole problem for adhoc on-demand distance vector routing protocol. One limitation of the proposed method is that it works based on an assumption that malicious nodes do not work as a group, although this could happen during a real scenario and presently gazing this downside of team attacks.

Xue and Nahrstedt (2004) proposed a new routing service named best-effort fault-tolerant routing (BFTR). The design goal of BFTR is to provide packet routing service with high delivery ratio and low overhead in presence of misbehaving nodes. Instead of identifying whether a path is good or bad, i.e., whether it contains any misbehaving node, BFTR evaluates the routing feasibility of a path by its end-to-end performance (e.g. packet delivery ratio and delay).

By continuously observing the routing performance, BFTR dynamically routes packets via the most feasible path. BFTR provides an efficient and uniform resolution for a broad range of node misbehaviors with very few security assumptions. The BFTR algorithm is evaluated through both analysis and extensive simulations. The results show that BFTR greatly improves the adhoc routing performance in the presence of misbehaving nodes.

Baadache and Belmehdi (2010) proposed that after having specified the black hole attack, a secure mechanism, which consists in checking the good forwarding of packets by an intermediate node. The proposed solution avoids the black hole and the cooperative black hole attacks. Evaluation metrics

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

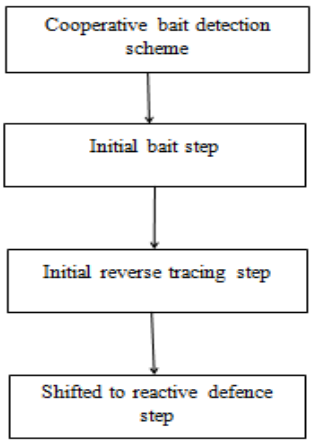
were considered in simulation to show the effectiveness of the suggested solution.

III.PROPOSED WORK

The proposed methodology presents 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 this 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 therefore the superiority of reactive response at the following steps so as to scale back the resource wastage.

The CBDS scheme (Jian-Ming Chang et al.,2015) comprises three steps

1) The initial bait step
2) The initial reverse tracing step
3) The shifted to reactive defense step

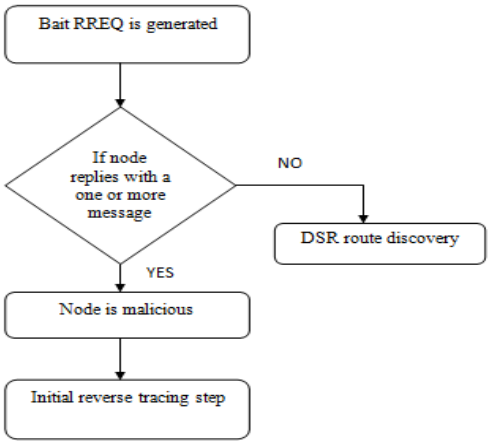


THE INTIAL BAIT STEP

The goal of the bait phase is to simulate 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 meant to get the destination address of the bait RREQ .The source node stochastically selects an adjacent node, within its one-hop neighbourhood nodes and cooperates with this node by taking its address as the destination address of the bait RREQ. First, if the neighbour 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 neighbour 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 neighbour node had sent the reply RREP, it means that there was no other malicious node present within the network. Hence CBDS had initiated the DSR route discovery phase.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017



INTIAL REVERSE TRACING STEP

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 within the route. It should be emphasised that the CBDS is able to detect more than one malicious node simultaneously when these nodes send reply RREPs. When malicious node nm replies with the false RREP, an address list P = $\{n_1,.....n_k,.....n_m,....n_r\}$ is recorded. If node n_k receives the RREP, it will separate the P list by the destination address n1 and address list becomes Kk = $\{n_1,.....n_k\}$. The difference in the address feild is calculated as

$$Kk' = P- Kk$$

Result is stored in RREP's "Reserved field".

Suspicious path information S replied by malicious node is detected

$$S = K1' \cap K2' \cap K3' ..... \cap Kk'$$

The set difference operation of P and S is conducted to acquire a temporarily trusted set

$$T = P - S$$

The source node would send test packets to this route and would send the recheck message to second node towards the last node in T.

SHIFTED TO REACTIVE DEFENSE STEP

In this step, the DSR route discovery process is activated. When the route is established and if at the destination, it is found that the packet delivery ratio has significantly falls to the threshold, the detection scheme would be triggered again for continuous maintenance and real-time reaction efficiency. The threshold may be a changing value in the range 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 within the network. In that case, the threshold should be adjusted upward. Otherwise, the threshold will be lowered.

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 ;
```

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

```
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 ;
}
```

Security schema

In this ACBDS additional security feature is added. Encryption of messages are done. Hence the attacker can not gain necessary information in the network environment.

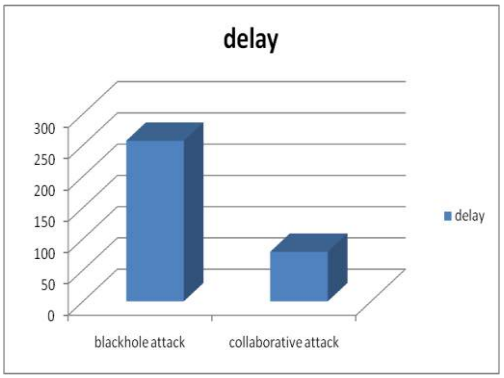
IV.PERFORMANCE METRICS

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 d_i, and the number of packets received by the destination node is $pktd_i$. The average end-to-end delay of the application traffic n, which is denoted by E, is obtained as

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

Delay is the difference between the time at which the sender generated the packet and the time at which the receiver received the packet. Delay is calculated using awk script which processes the trace file and produces the result.



In this graph, the delay in the presence of blackhole attack and collaborative attack are compared. The delay occurs due to some network errors.

Throughput

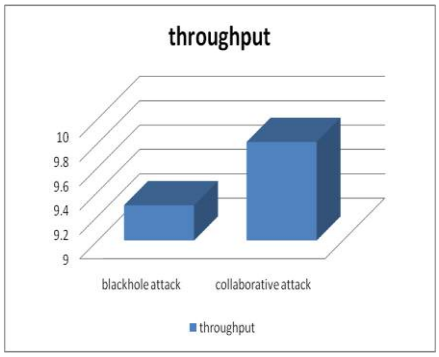
This is defined as the total amount of data (bi) that the destination receives them from the source divided by the time (ti) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput of the application traffic n, which is denoted by T, is obtained as

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

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

Throughput is the number of successfully received packets in a unit time and it is represented in bps. Throughput is calculated using awk script which processes the trace file and produces the result.



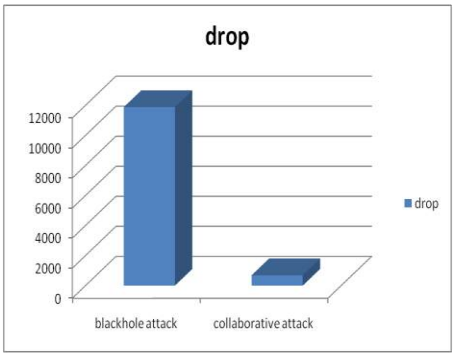
In this graph, the throughput in the presence of blackhole attack and collaborative attack are compared. This occurs due to some network errors also.

Packet Drop

Packet loss in a communication is the difference between the generated and received packets. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet Loss is calculated using awk script which processes the trace file and produces the result.

Packet drop = GeneratedPackets – ReceivedPackets

Where generatedpackets is the number of packets generated to transmit and the receivedpackets is the number of received packets which are transmitted.



In this graph, the packet drop in the presence of blackhole attack and collaborative attack are compared. This occurs due to some network errors also.

RESULT

Simulation Scenario

Scenario 1

Here only one malicious node is considered for routing protocols like DSR and AODV

Scenario 2

Here only two malicious node is considered for routing protocols like DSR and AODV

Table 4.1 comparison between DSR and AODV

Parameter/Protocol	DSR		AODV	
	Scenario 1	Scenario 2	Scenario 1	Scenario 2
Delay	463.054	338.921	153.184	156.57
Throughput	19.04	17.87	22.12	18.62
Dropped Packets	4582	9184	4576	9150

Considering such scenarios the performance metrics such as delay, throughput and packet drop are calculated. These values are calculated form the

awk script in ns2 simulator. Awk script is one of the most prominent text-processing utility on GNU/Linux. It can solve complex text processing tasks with a few lines of code. Using this script, the values for the drop, throughput and delay are generated and are plotted in the form of graph. From the above observations, AODV protocol is more efficient. Hence this routing protocol is used for further implementation.

V.CONCLUSION AND FUTURE WORK

In this work, a new mechanism called the CBDS for detecting malicious nodes in MANETs under collaborative black hole and rushing attacks. These networks are subjected to black hole and rushing attacks. Any detected malicious node is kept in a malicious 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.

In an attempt to find a lasting solution to the security challenges in MANETs, various researchers have proposed different solutions for various security issues in MANETs. Identifying a malicious node in a network has been a reoccurring challenge. Since there is no particular line of defense, security for MANETs is still a major concern. This approach is based on using cooperative bait detection scheme to detect and prevent black hole attacks in MANETs.

This mechanism is extended against coḷlaborative attacks such as rushing and black hole attack.

REFERENCES

[1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach",IEEE sustems journal,vol. 9, NO. 1, MARCH 2015

[2] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chenai, India, Feb. 28–Mar., 03, 2011, pp. 1–5

[3] 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.

[4] H. Deng, W. Li, and D. Agrawal, "Routing Security in Wireless Adhoc Network," IEEE Commun. Mag., vol. 40, no. 10, Oct. 2002.

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

[6] W. Kozma and L. Lazos, "REAct: resource-efficient accountability for node misbehavior in Adhoc networks based on random audits", in Proc. WiSec, 2009, pp. 103–110.

[7] Nai-wei lo, Fang-ling liu, "a secure routing protocol to prevent cooperative blackhole attack in MANET", intelligent technologies and engineering systems, lecture notes in electrical engineering ,volume 234, 2013, pp 59-65.

[8] 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.

[9] 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.

ISSN (ONLINE): 2395-695X
ISSN (PRINT): 2395-695X

International Journal of Advanced Research in Basic Engineering Sciences and Technology (IJARBEST)
Vol.3, Special Issue.24, March 2017

[10] S. Corson and J. Macker, RFC 2501, "Mobile Adhoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", Jan. 1999.

[11] IEEE Standard for Information Technology, IEEE Std 802.11-14997, 1997, Telecommunications and Information exchange between systems: wireless LAN medium access control (MAC) and physical layer (PHY) Specifications, pp. i-445.

[12] P.Manickam, T.Guru baskar, M.Girija, Dr.D.Manimegalai, "Performance comparisons of Routing Protocols in Mobile Ad-Hoc Networks", international journal of wireless & mobile networks (ijwmn) vol. 3, no. 1, February 2011.