IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

Mitigation of Cooperative Black Hole Attack and Rushing Attack in MANETS

Gowri S[1], M/S. Lipsa Dash[2]

Final Year M.Tech-Communication Systems, New Horizon College of Engineering, Bangalore[1]

Asst. Professor, ECE Dept, New Horizon College of Engineering, Bangalore[2]

Abstract: A Mobile ad hoc network (MANET) is a kind of network where the mobile devices are with a dynamic structure. Here each node in the network participates in routing by forwarding data packets to other nodes. Security becomes a crucial concern to ensure protected communication between nodes in ad hoc networks. There are several of challenges with respect to security design as ad hoc network is a decentralized and infrastructure less type of wireless network. There are five layers in MANET and each of these layers is prone to various kinds of attacks. This paper discusses about two important attacks in network layer, their defence mechanisms, those are: Cooperative Black Hole Attack and Rushing Attack. Mobile ad hoc networks (MANETs) are mostly and widely used in military and civilian applications. Due to the dynamic topology of MANETs, it allows the nodes to join and leave the network at any point of time. This generic characteristic of MANET is a cause which makes it vulnerable to security attacks. In this paper, I address the problem of coordinated attack by multiple black holes acting in group and rushing attack. I introduce a technique to identify multiple black hole nodes cooperating with each other and rushing nodes and solutions to discover a safe route avoiding cooperative black hole attack and rushing attack.

Keyword: MANET, Destination Sequenced Distance Vector routing (DSDV), Dynamic Source Routing (DSR).

1. INTRODUCTION

Ad hoc wireless networks have a large number of potential applications. In Military application Ad hoc networks are used in connecting soldiers or other military units to each other on the battlefield or creating sensory arrays with thousands of sensors are two crucial examples. The concept of Ad hoc networks arises when we need to create a network in situations where establishing the infrastructure would be highly impossible or probably expensive. As we all know with the case of fixed infrastructure where mobile nodes communicates via base station but in Adhoc networks, mobile nodes do not communicate via access points (fixed structures). Each mobile node in Adhoc networks plays two important roles:
1) Acts as a host when requesting or providing information from or to other nodes in the network, and
2) Also acts as router while discovering and maintaining routes for other nodes in the network.
Ad hoc networks have a large number of potential applications. Military uses such as connecting soldiers or other military units to each other on the battlefield or creating sensory arrays with thousands of sensors are two typical examples. Ad hoc networks provide a possibility of creating a network in situations where creating the infrastructure would be impossible or prohibitively expensive. Unlike a network with fixed infrastructure, mobile nodes in ad hoc networks do not communicate via access points (fixed structures). Each mobile node acts as a host when requesting/providing information from/to other nodes in the network, and acts as router when discovering and maintaining routes for other nodes in the network.

There are currently three main routing protocols for ad hoc networks [1], DestinationSequenced Distance Vector routing (DSDV) [12], Dynamic Source Routing (DSR) [9], and AODV [2]. DSDV is a table driven routing protocol. In DSDV, each mobile node in the network maintains a routing table with entries for every possible destination node, and the number of hops to reach them. The routing table is periodically updated for every change in the network to maintain consistency. This involves frequent route update broadcasts. DSDV is inefficient because as the network grows the overhead grows as O(n2) [1]. DSR is an on-demand routing protocol and it maintains a route cache, which leads to memory overhead. DSR has a higher overhead as each packet carries the complete route, and does not support multicast. AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself. Each intermediate node receiving the RREQ, makes an entry in its routing table for the node that forwarded the RREQ message, and the source node. The destination node or the intermediate node with a fresh enough route to the destination node, unicasts the Route Response (RREP) message to the

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

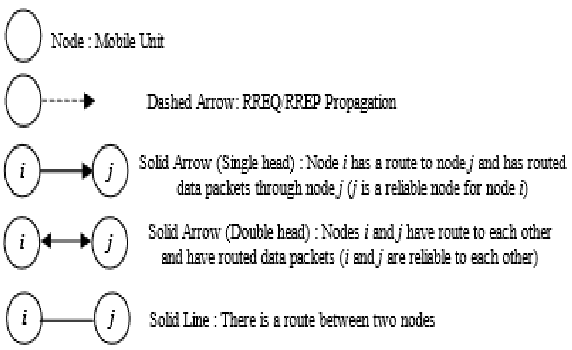
neighboring node from which it received the RREQ. An intermediate node makes an entry for the neighbouring node from which it received the RREP, then forwards the RREP in the reverse direction. Upon receiving the RREP, the source node updates its routing table with an entry for the destination node, and the node from which it received the RREP. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP.

Some researchers [3-8, 10-11] discuss the vulnerabilities in Ad hoc routing protocols and the attacks that can be mounted. The AODV protocol is vulnerable to the well-known black hole attack. A black hole is a node that always responds positively with a RREP message to every RREQ, even though it does not really have a valid route to the destination node. Since a black hole does not have to check its routing table, it is the first to respond to the RREQ in most cases. When the data packets routed by the source node reach the black hole node, it drops the packets rather than forwarding them to the destination node. Deng, Li, and Agrawal [3] assume the black hole nodes do not work as a group and propose a solution to identify a single black hole. However, the proposed method cannot be applied to identifying a cooperative black hole attack involving multiple nodes. In this paper, we develop a methodology to identify multiple blackhole nodes cooperating as a group. The technique works with slightly modified AODV protocol and makes use of the Data Routing Information (DRI) table in addition to the cached and current routing tables.

2. COOPERATIVE BLACK HOLE ATTACK PROBLEM

2.1 Black Hole

A black hole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. We define the following conventions for protocol representation.



2.2 Cooperative Black Hole Attack

According to the original AODV protocol, when source node S wants to communicate with the destination node D, the source node S broadcasts the route request (RREQ) packet. The neighboring active nodes update their routing table with an entry for the source node S, and check if it is the destination node or has a fresh enough route to the destination node. If not, the intermediate node updates the RREQ (increasing the hop count) and floods the network with the RREQ to the destination node D until it reaches node D or any other intermediate node which has a fresh enough route to D, as depicted by example in Figure 1. The destination node D or the intermediate node with a fresh enough route to D, initiates a route response (RREP) in the reverse direction, as depicted in Figure 3. Node S starts sending data packets to the neighboring node which responded first, and discards the other responses. This works fine when the network has no malicious nodes.

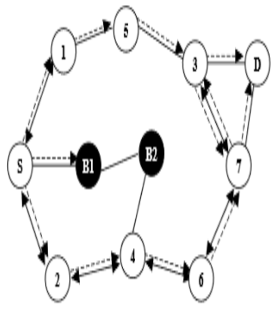


Figure 1: Network flooding of RREQ

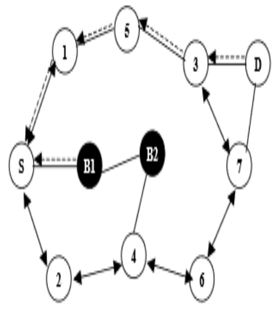


Figure 2: Propagation of RREP messages

Researchers have proposed solutions to identify and eliminate a single black hole node [3]. However, the case of multiple black hole nodes acting in coordination has not been addressed. For example, when multiple black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its teammates B2 as the next hop, as depicted in Figure 2. According to [3], the source node S sends a “Further Request (FRq)” to B2 through a different route (S-2-4-B2) other than via B1. Node S asks B2 if it has a route to node B1 and a route to destination node D. Because B2 is cooperating with B1, its “Further Reply (FRp)” will be “yes” to both the questions. Now per the solution proposed in [3], node S starts passing the data packets assuming that the route S-B1-B2 is secure. However, in reality, the packets are consumed by node B1 and the security of the network is compromised.

3. RUSHING ATTACK

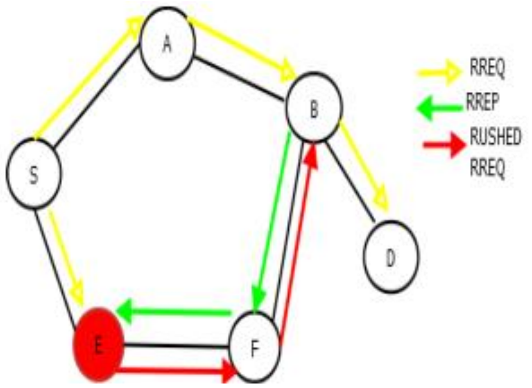
One of the property of an on-demand routing protocol is that nodes are only allowed to forward the first RREQ that arrives for routing discovery and it discards all other RREQ that come late. This property is exploited by rushing attack. The attacker will transmit the RREQ request earlier and thus it suppresses the legitimate RREQ. In most powerful rushing attack they use a wormhole to rush packets.

For example, in figure the node “E” represents the rushing attack node, where “S” and “D” refers to source and destination nodes. The rushing attack of compromised node “E” quickly broadcasts the route request messages to ensure that the RREQ message from itself arrive earlier than those from other nodes. This result in when “C” i.e. neighbouring node of “D” when get the legitimate route request from source, they simply ignore the request. So in the presence of such attacks “S” fails to discover any

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

useable route or safe route without the involvement of attacker.



4. SOLUTION FOR COOPERATIVE BLACK HOLE ATTACK

In this section, we propose a methodology for identifying multiple black hole nodes cooperating as a group with slightly modified AODV protocol by introducing Data Routing Information (DRI) Table and Cross Checking.

4.1 Data Routing Information Table

The solution to identify multiple black hole nodes acting in cooperation involves two bits of additional information from the nodes responding to the RREQ of source node S. Each node maintains an additional Data Routing Information (DRI) table. In the DRI table, 1 stands for 'true' and 0 for 'false'.

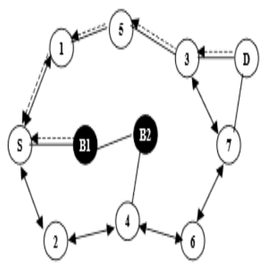


Figure 3: Solution to avoid cooperative black hole attack

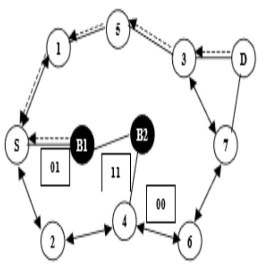


Figure 4: Solution to identify multiple black hole nodes in one-time check

The first bit "From" stands for information on routing data packet from the node (in the Node field) while the second bit "Through" stands for information on routing data packet through the node (in the Node field). In reference to the example of Figure 3, a sample of the database maintained by node 4 is shown in Table 1.

Node #	Data Routing Information	
	From	Through
3	1	0
6	1	1
B2	0	0
2	1	1

Table 1. Additional table of data routed from, and routed to nodes maintained by node 4

The entry 1 0 for node 3 implies that node 4 has routed data packets from 3, but has not routed any data packets through 3 (before node 3 moved away from 4). The entry 1 1 for node 6 implies that, node 4 has successfully routed data packets from and through node 6. The entry 0 0 for node B2 implies that, node 4 has NOT routed any data packets from or through B2.

4.2 Cross Checking

In our techniques we rely on reliable nodes (nodes through which the source node has routed data) to transfer data packets. The modified AODV protocol, and the algorithm for our proposed methodology are illustrated in Figure 5. In the protocol, the source node (SN) broadcasts a RREQ message to discover a secure route to the destination node. The Intermediate Node (IN) generating the RREP has to provide its Next Hop Node (NHN), and its DRI entry for the NHN. Upon receiving RREP message from IN, the source node will check its own DRI table to see whether IN is a reliable node. If source node has used IN before to route data, then IN is a reliable node and source node starts routing data through IN. Otherwise, IN is unreliable and the source node sends FRq message to NHN to check the identity of the IN, and asks NHN: 1) if IN has routed data packets through NHN, 2) who is the current NHN's next hop to destination, and 3) has the current NHN routed data through its own next hop. The NHN in turn responds with FRp message including 1) DRI entry for IN, 2) the next hop node of current NHN, and 3) the DRI entry for the current NHN's next hop. Based on the FRp message from NHN, source node checks whether NHN is a reliable node or not. If source node has routed data through NHN before, NHN is reliable; otherwise, unreliable.

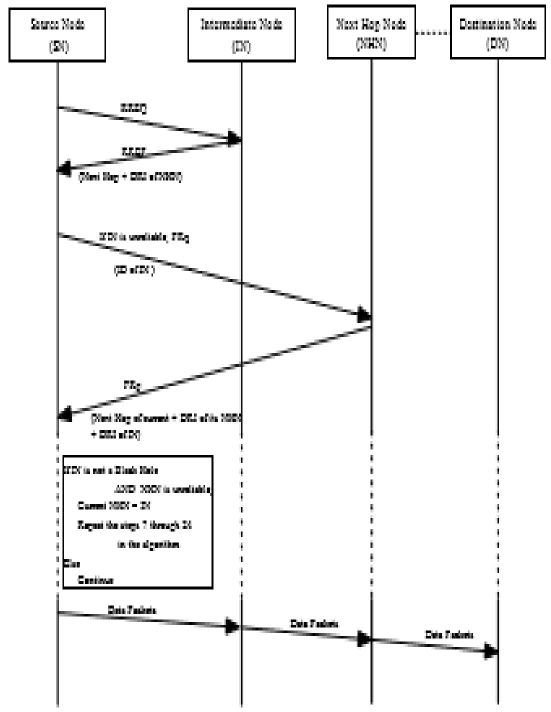
If NHN is reliable, source node will check whether IN is a black hole or not. If the second bit (ie. IN has routed data through NHN) of the DRI entry from the IN is equal to 1, and the first bit (ie. NHN has routed data from IN) of the DRI entry from the NHN is equal to 0, IN is a black hole. If IN is not a black-hole and NHN is a reliable node, the route is secure, and source node will update its DRI entry for IN with 01, and starts routing data via IN. If IN is a black-hole, the source node identifies all the nodes along the reverse path from IN to the node that generated the RREP as black hole nodes. Source node ignores any other RREP from the black holes and broadcasts the list of cooperative black holes. If NHN is an unreliable node, source node treats current NHN as IN and sends FRq to the updated IN's next hop node and goes on in a loop from steps 7 through 24 in the algorithm.

As an example, let's consider the network in Figure 4. When node B1 responds to source node S with RREP message, it provides its next hop node B2 and DRI for the next hop (i.e. if B1 has routed data packets through B2). Here the black hole node lies about using the path by replying with the DRI value equal to 0 1. Upon receiving RREP message from B1, the source node S will check its own DRI table to see whether B1 is a reliable node. Since S has never sent any data through B1 before, B1 is not a reliable node to S.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016



Algorithm to prevent cooperative black hole attack in MANETs

Notations :

SN: Source Node IN: Intermediate Node
DN: Destination Node NHN: Next Hop Node
FRq: Further Request FRp: Further Reply
Reliable Node: The node through which the SN has routed data
DRI: Data Routing Information
ID: Identity of the node

```
1   SN broadcasts RREQ
2   SN receives RREP
3   IF (RREP is from DN or a reliable node) {
4       Route data packets (Secure Route)
5   }
6   ELSE {
7       Do {
8           Send FRq and ID of IN to NHN
9           Receive FRp, NHN of current NHN, DRI entry for
10                  NHN's next hop, DRI entry for current IN
11          IF (NHN is a reliable node) {
12              Check IN for black hole using DRI entry
13              IF (IN is not a black hole)
14                  Route data packets (Secure Route)
15              ELSE {
16                  Insecure Route
17                  IN is a black hole
18                  All the nodes along the reverse path from IN to the node
19                          that generated RREP are black holes
20              }
21          }
22          ELSE
23              Current IN = NHN
24      } While (IN is NOT a reliable node)
25  }
```

Figure 5: Modified AODV protocol and algorithm to prevent cooperative black hole attack

Then S sends FRq to B2 via alternative path S-2-4-B2 and asks if B2 has routed any data from B1, who is B2's next hop, and if B2 has routed data packets through B2's next hop. Since B2 is collaborating with B1, it replies positively to all the three requests and gives node 6 (randomly) as its next hop. When the source node contacts node 6 via alternative path S-2-4-6 to cross check the claims of node B2, node 6 responds negatively. Since node 6 has neither a route to node B2 nor has received data packets from node B2, the DRI value corresponding to B2 is equal to 0 0 as shown in Figure 4. Based on this information, node S can infer that B2 is a black hole node. If node B1 was supposed to have routed data packets through node B2, it should have validated the node before sending it. Now, since node B2 is invalidated through node 6, node B1 must cooperate with node B2. Hence both nodes B1 and B2 are marked as black hole nodes and this information is propagated through the network leading to their listing as black holes, and revocation of their certificates. Further, S discards anyfurther responses from B1 or B2 and looks for a valid alternative route to D.

The process of cross checking the intermediate nodes is a onetime procedure which we believe is affordable to secure a network from multiple black hole nodes. The cost of cross checking the nodes can be minimized by letting nodes sharing their trusted nodes list (DPI table) with each other

5. SOLUTION FOR RUSHING ATTACK

Source route delegation mechanism is used to verify that all the secure neighbour detection procedure are performed between two neighbouring nodes. To explain the mechanism let us consider two neighbouring node n1 and n2,here n1 gets a route request from node S with sequence id, that is destined to node R. Node n1 does the neighbouring detection protocol and find that n2 is the neighbouring node that is within range and then it delegates the route request to n2.The delegation of route request to n2 is given as follows:

MA = (ROUTE DELEGATION; A; B; S; R; id)
MA = Sign (H (MA))
A->B: (MA)

Here node n2 can rebuilt the message fields and verify the signature. The node n2 will accept the route delegation if n2 find n1 within the range and this procedure is done to next neighbours and so on. The route delegation message can be incorporated with the last message of secure neighbour detection protocol.

6. SIMULATION PARAMETERS

Protocol used: AODV
Channel type: Wireless Channel
Number of Nodes: 11 Nodes (For cooperative black hole attack)
6 Nodes (For rushing attack)
Number of malicious nodes: 2 Nodes (For cooperative black hole attack)
1 Node (For rushing attack)
Simulation Time: 32.5 (For cooperative black hole attack)
20.0 (For rushing attack)

8. Simulation results

Control over head: Control over head is more in cooperative black hole attack compared to rushing attack as the additional two bit are added in routing table in case of cooperative black hole attack.

DOI 10.17148/IJARCCE.2016.55234

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

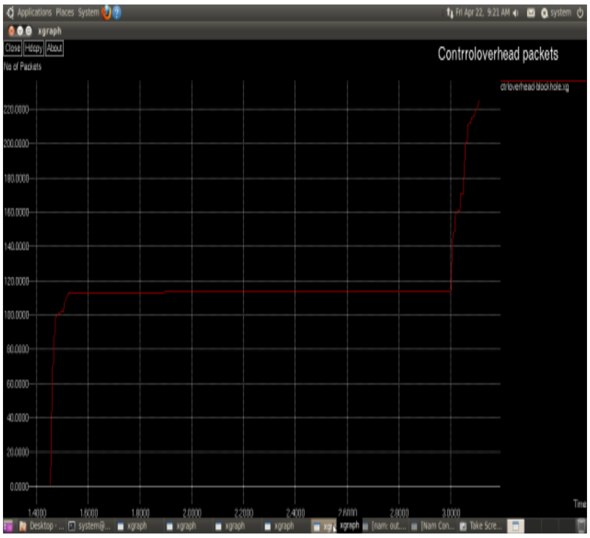


Fig 6: Control over head for Cooperative black hole attack.

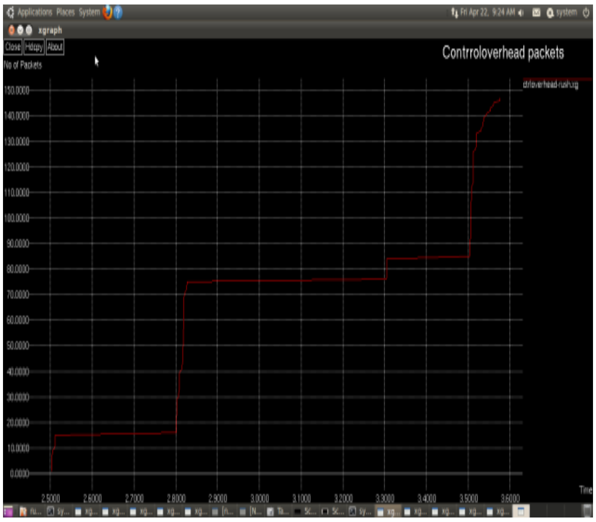


Fig 7: Control over head for rushing attack

Delay: Given by the difference between received time and transmitted time of data packets.

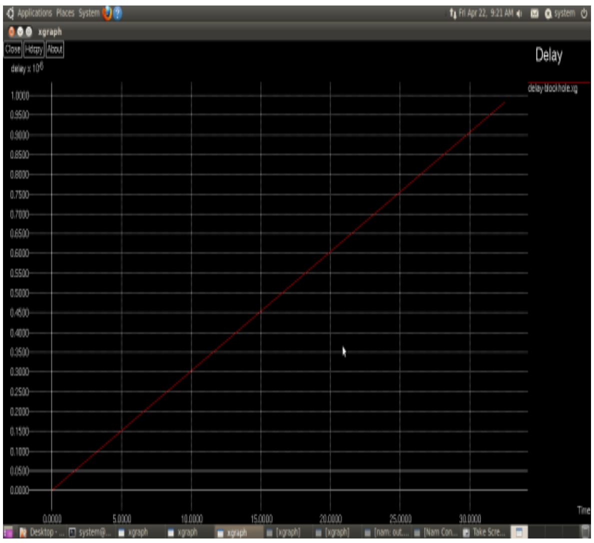


Fig 8 Delay for Cooperative black hole attack

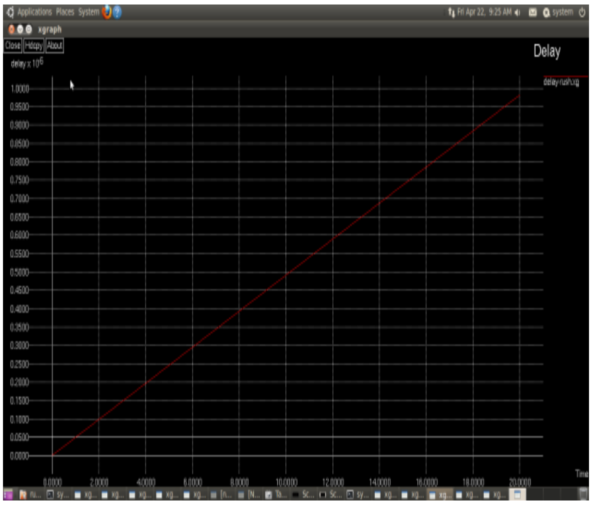


Fig 9: Delay for rushing attack

Throughput: Through is calculated by the sum of sent packets and received packets with respect to time.

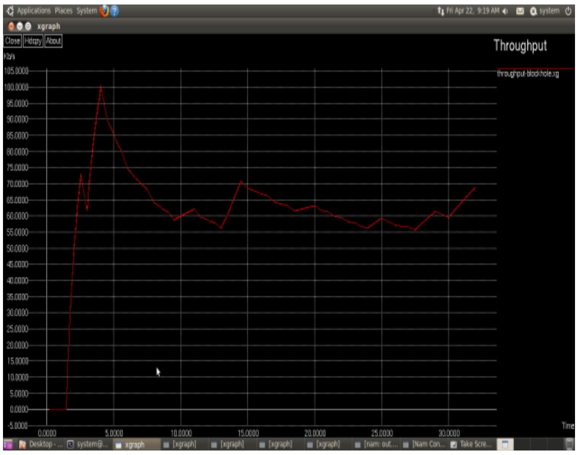


Fig 10: Throughput for Cooperative black hole attack

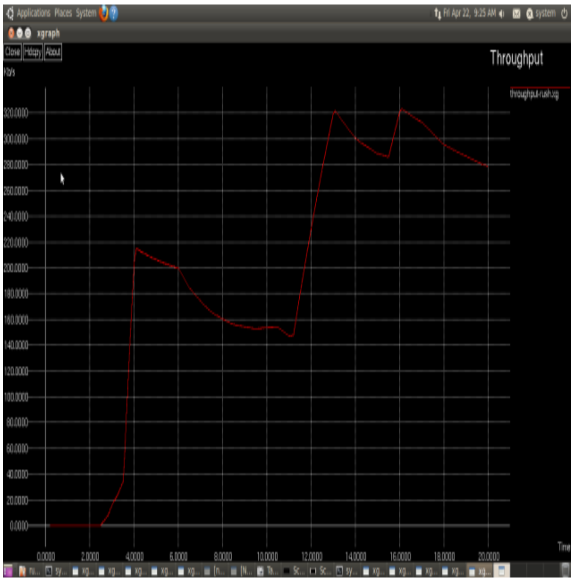


Fig 11: Throughput for rushing attack

Packet delivery ratio: Defined by the ratio of received packets to sent packets.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 5, May 2016

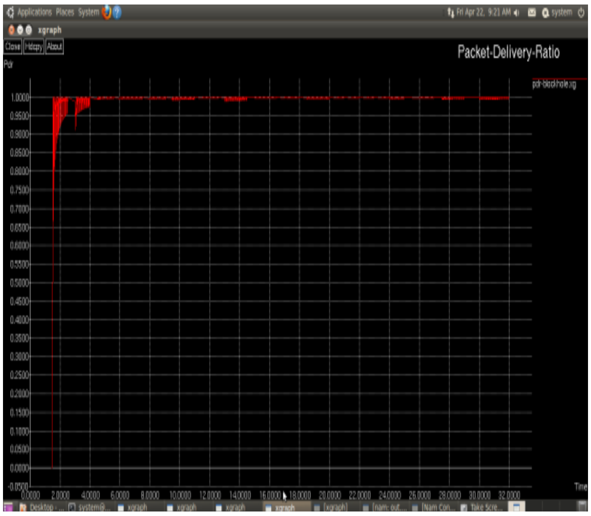


Fig 12: Packet delivery ratio for Cooperative black hole attack

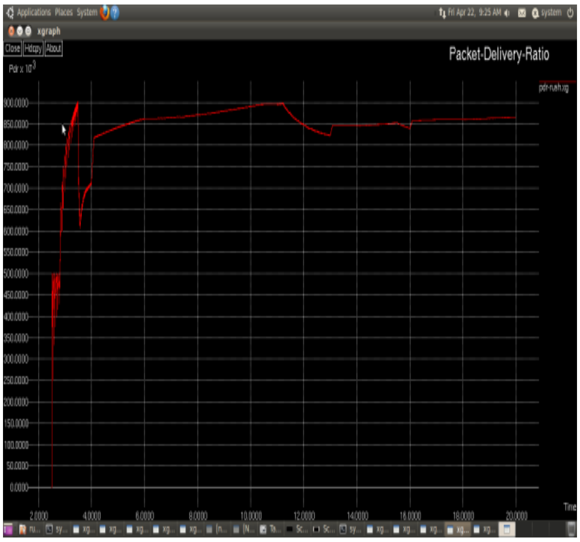


Fig 13: Packet delivery ratio for rushing attack

Bit error rate: Defined as the number of packet dropped with respect to time.

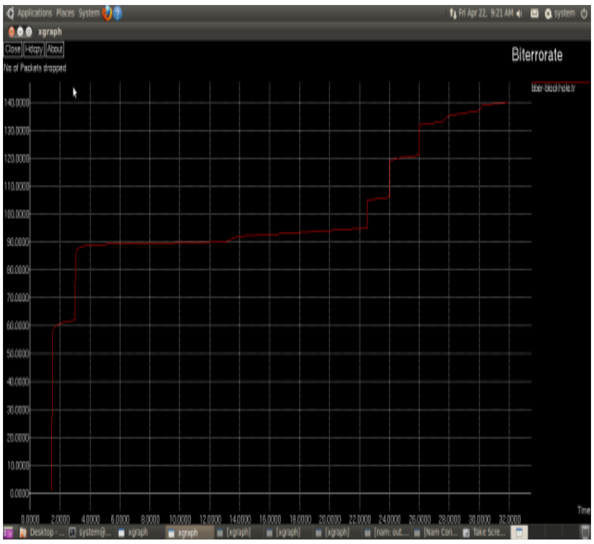


Fig 14: Bit error rate for Cooperative black hole attack

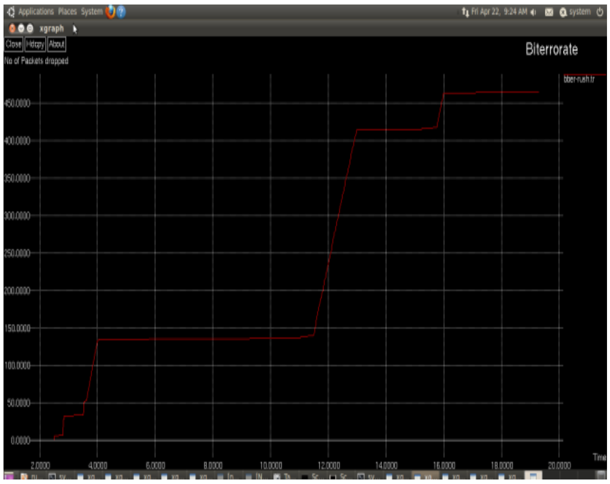


Fig 15: Bit error rate for rushing attack

7. CONCLUSION

In this paper we have studied the routing security issues of MANETs, described the cooperative black hole attack and rushing attack that can be mounted against a MANET and proposed a feasible solution for it in the AODV protocol. The proposed solution can be applied to 1.) Identify multiple black hole nodes cooperating with each other in a MANET; 2.) Discover secure paths from source to destination by avoiding multiple black hole nodes acting in cooperation;3.) Identify rushing node; 4.) Avoiding rushing attack and identifying a secure path.

REFERENCES

[1] Elizabeth M. Royer, and Chai-KeongToh, “A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks,” IEEE Personal Communications, pp. 46-55, April 1999.

[2] Charles E. Perkins, and Elizabeth M. Royer, “Ad-hoc On-Demand Distance Vector (AODV) Routing,” Internet Draft, November 2002.

[3] Hongmei Deng, Wei Li, and Dharma P. Agrawal, “Routing Security in Wireless Ad Hoc Network,” IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[4] S. Marti et al., “Mitigating Routing Misbehavior in Mobile Ad Hoc Networks,” 6th Int’l. Conference Mobile Comp. Net., pp. 255-265, August 2000.

[5] VesaKärpijoki, “Security in Ad hoc Networks,” http://www.tcm.hut.fi/Opinnot/Tik110.501/2000/papers/karpijoki.pdf.

[6] SrdjanCapkuny, LeventeButty´an, and Jean-Pierre Hubaux, “Self-Organized Public-Key Management for Mobile Ad Hoc Networks,” Technical Report at EPFL, http://ic2.epfl.ch/publications/documents/IC_TECH_REPORT_200234.pdf.

[7] Lidong Zhou, and Zygmunt J. Haas, “Securing Ad Hoc Networks,” IEEE Network Magazine, vol. 13, no.6, November/December 1999.

[8] Janne Lundberg, “Routing Security in Ad Hoc Networks,” http://citeseer.nj.nec.com/cache/papers/cs/19440/http:zSzzSzwww.tml.hut.fizSz~jluzSznetseczSz netsec-lundberg.pdf/routing-security-in-ad.pdf

[9] David B. Johnson, and David A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks,” Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[10] Y. Zhang, W. Lee, “Intrusion Detection in Wireless Ad Hoc Networks,” 6th Int’l. Conference Mobile Comp. Net., Mobicom 2000, pp. 275-283, August 2000.

[11] HaiyunLuo, PetrosZerfos, Jiejun Kong, Songwu Lu and Lixia Zhang, “Self-securing Ad Hoc Wireless Networks,” http://www.cs.ucla.edu/~jkong/publications/ISCC02.pdf.

[12] C. E. Perkins and P. Bhagwat, “Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers,” Computer Communications Review, pp. 234-244, October 1994.