Asian Journal of Information Technology 15 (4): 694-702, 2016
ISSN: 1682-3915

An Analytical Approach to Detect and Isolate Attacks in Mobile Adhoc Networks Using Cross Layer Feedback

[1]G. Usha, [2]S. Kannimuthu, [3]M. Karthi and [4]J. Joshua
[1]Department of Information Technology, Karpagam College of Engineering,
[2]Department of CSE, Karpagam College of Engineering,
[3]Department of Information Technology, Karpagam College of Engineering, Coimbatore, India
[4]Department of Software Engineer, ETL-Developer Build, Preludesys India Ltd., Chennai, India

Abstract: Mobile Adhoc Network (MANET) is a self-organizing network consists of wireless mobile devices. In this study, we detect and isolate one particular type of attack known as black hole attack. Black hole attack is one of the most vulnerable attacks for MANET. In this study, an analytical model is also proposed to detect attacks. We adopted dynamic cross layer feedback technique to detect and isolate the attack. The proposed architecture uses three types of major parts known as cross layer feedback, detection and isolation. The proposed methodology is compared with existing methodology. Analytical and simulation results show that the proposed methodology performs well and improves packet delivery ratio and reduces packet drop ratio in dynamic changing MANET environment. Network overhead is also greatly reduced.

Key words: Mobile Adhoc Network (MANET), cross layer, black hole attack, Adhoc On Demand Distance Vector (AODV), PMC

INTRODUCTION

Mobile Adhoc network is a type of wireless network in which the topology of mobile adhoc network changes dynamically. So, providing security to these networks is a challenging issue (Yang *et al*., 2004; Burbank *et al*., 2006; Zhou and Haas, 1999). The attackers can easily eavesdrop the network and drop packets. Black hole attack is one type of denial of service attack where the malicious node invades the network and drops the packets (Joseph *et al*., 2007). In most current solutions to detect black hole attacks only routing layer information is considered to detect attacks. Cross layer based security is the future scope of wireless networks. Because single layer solutions used to detect attacks in wireless networks are failed in many scenarios.

Traditional wired networks use only single layer information to detect attacks. But due to mobility, interference, dynamic topology, connection less nature the single layer security solution is not sufficient to provide complete security to MANET (John *et al*., 2007). Hence, a cross layer (Milanovic *et al*., 2004; Kannhavong *et al*., 2007) approach is necessary to provide more security to MANET. So in our proposed approach, MAC layer and routing layer metrics are used to detect and isolate attacking nodes from the network. MAC layer is responsible for establishing a reliable and secure link. So, MAC layer parameters as well as routing layer parameter are used. This research also uses an analytical model to detect the black hole attacks on adhoc networks. The results of analytical model are compared with the help of simulation experiment in order to examine the proposed technique.

The primary objective is to demonstrate an efficient approach to detect and isolate black hole attacks from MANET. The proposed algorithm is simple and fast. Since, this approach use only a single packet to detect attacks. In this study, we also propose an efficient cross layer architecture which uses the cross layer feedback information. By using this cross layer feedback it efficiently detects the black hole attacks in MANET. Experimental evaluation and analytical model proofs show that the proposed solution detects attack and packet delivery ratio also increased in the presence of black hole nodes in the network efficiently. Packet drop ratio is greatly reduced and network overhead also reduced.The rest of this study is organized as follows.

Literature review: In literature, various authors proposed solutions to defend against black hole attacks in

Corresponding Author: G. Usha, Department of Information Technology, Karpagam College of Engineering, Chennai, India

MANET. We classify our related work based on single layer detection and cross layer detection technique.

Single layer design: Many researchre proposed solutions to detect black hole attacks in MANET. There are various secure routing protocols such as Secure Adhoc On demand Distance Vector routing (SAODV) (Lu *et al*., 2009). Al-Shurman *et al*. (2004) propose two different types of solution to defend against black hole attack. The first method, works in redundant route identification technique. In this approach, the researcher assumed that there is more than one path available for a source node to transfer packets. The source node recognizes the safe route by considering the number of hops or nodes which avoids routing through black hole attacks. In second solution, by using the sequence number they identified the attacks. This approach contains additionally two tables which maintain the details about last packet sequence number and last packet received. By using this information the sender node identifies the malicious node. Tamilselvan and Sankaranarayanan (2007) propose the detection technique by using a timer which is in timer expired table. It collects the request from all the nodes and stores the sequence number which is named as Collect Route Reply Table (CRRT). Based on the time out value, it judges the route. Because of setting the timer, the communication delay increases in the network. Jaisankar *et al*. (2010) the propose security technique consist of two parts such as detection and reaction part. In detection part each node maintains a Black Identification Table (BIT) which stores information's like source id, destination id, Packet Modified Count (PMC), Packet Received Count (PRC), Packet Forwarded Count (PFC). By using the PMC and the BIT table is updated for black hole nodes. Next part is reaction part where the nodes are isolated by maintaining isolation table. The isolation table also stores the ID's of black hole nodes which are broadcasted to all other nodes in the network. Delay is introduced in the network. Mistry *et al*.(2010) propose detection technique maintains additionally three fields. They are Cmg_RREP_Tab, a timer MOS_WAIT_TIME and a Mali_node. The Cmg_RREP_Tab maintains the details about the received RREP's from received neigh-bors. MOS_WAIT_TIME is the timer where the source node waits for RREP packets from neighbors. The node which has highest sequence number is marked as malicious and stored in Mali_node. This field is maintained in order to identify the malicious node in future. Su (2011) propose scheme involves anti black hole mechanism for each nodes in the network. This technique additionally uses two tables which are RQ table and SN table. In the RQ table, it records the details about the RREQ messages within the transmission range of the communication area. The SN table records the suspicious value of each node. The suspicious value is calculated by counting the number of forwarded RREQ messages by each node. If a node is not transmitting RREQ packets for a particular threshold value it is marked as malicious node. All the approaches presented above to detect black hole attack uses only single layer information. Not only that each technique presented above has its own pros and cons.

All the above researches used only single layer information to detect attacks. These solutions introduce additional overhead by introducing new tables and fields. But our proposed approach uses cross layer information. Even though, we are using cross layer parameters the network overhead is greatly reduced. Next we discuss few cross layer work carried in literature which inspired us to propose our solution. Only little work has been carried out in literature which uses cross layer information against attacks in MANET. Now, we discuss those researches in detail.

Cross layer design: Thamilarasu and Sridhar (2012) propose a cross layer based solution to detect jamming attacks in MANET. They used MAC layer as well as routing layer parameters to detect attacks. In their technique, the output from the detection modules is combined with decision module. They used rule based system to detect attacks in the network. Joseph *et al*. (2008) propose an architecture known as CARDS. It uses SVM algorithm to reduce the data. This technique uses apriori algorithm to reduce the data set. They also used Fischer discriminant algorithm to classify attacks from the MANET. The authors used cross layer information to classify attacks. Cross layer correlation technique is implemented in their work. They have correlated MAC layer features with network layer.

Even though, we are using cross layer parameters the network overhead is greatly reduced. Various researchre proposed different types of solutions to detect black hole (Nadeem and Howarth, 2013; Pranusha and Murali, 2015) attack in MANET. But, the proposed technique uses analytical model based cross layer solution to detect black hole attacks in MANET.

Assumptons: In order for the proposed system to work some factors are concerned to be true. The assumptions of the systems are not unrealistic which can be easily realized in an adhoc environment:

- All packets in the MANET act as a router where each node forwards and receives packets. This is a reasonable assumption because there is no centralized access in MANET

- Every link between the nodes is bidirectional
- Nodes operate in promiscuous mode; they can listen to their neighbors in the transmission range
- The MANET consist of normal nodes, malicious node and black hole detector node. Black hole detector node is not a malicious node

MATERIALS AND METHODS

Analytical model: In this study, we discuss about analytical model to prove our approach. Let us take a directed graph G = (V, E) be an adhoc network. Let us assume the adhoc network consist of set of V vertices and E edges which can be represented as $V=\{V_1,V_2,\ldots\ldots..V_n\}$ and E is represented as $E=\{E_1,E_2,\ldots\ldots\ldots\ldots..E_n\}$. We are declaring node B is cut vertex node because it has minimum number or no link to other nodes in the network. Now the cut vertex $B\epsilon V$. Thus in this black hole, attack the cut vertex B creates the virtual link by sending Fake RREP message by advertising itself has had a higher sequence number than other nodes. According to the AODV protocol, the source node communicates via attacker node B to the destination node. Thus, the cut vertex node B becomes the part of the network. As a result, other normal nodes can't able to participate in the communication. In this way, the attacker node participates in normal routing process. In the above illustration we considered only one black hole node in the network. But, when there is more number of black hole nodes, this situation is denoted by:

$$\forall s \text{ Set } (s_1) \Leftrightarrow \exists B(\text{Black hole}(B)) \quad \text{where } B \in G \tag{1}$$

Now, let us take N be the subset of nodes which consist of source, destination nodes:

$$\forall s_1,s_2, s_2 \subseteq s_1 \Leftrightarrow \forall s (N \in s_1 \Rightarrow N \in s_2) \quad \text{where } N \in G \tag{2}$$

Assume $N \cap B = \{\Phi\}$. Let PFM (T_{hi}) denotes the threshold value for packet forwarded at MAC layer. Assume the route request message RRE_Q reaches every node in the network. In return, the normal nodes reply a route reply message $RREP_n$ and black hole node replies $RREP_B$ to the source node.

Lemma 1: If there is a black hole node in the network where by receiving RREQ messages, if the black hole node forwards same RREP messages again and again then the total forwarded packets will be more than the average forwarded threshold value in MAC layer.

Proof: Let PFM (T_{hi}) be a function that returns the packet forwarded threshold value from each node of MAC layer.

From the implementation of AODV, normally packets forwarded between source node destination nodes will be within the packet forwarded threshold value. Therefore, if the black hole node increases RREP message the threshold value increases if:

$$\text{PFM } (T_{hi}) > \text{RREP}_B \tag{3}$$

Therefore, when total number of forwarded packets ($RREP_B$) is more than the threshold calculated, there exists a black hole node in the network. Hence, the MAC layer feedback to network layer is set to true which can be denoted as $L(T_{hi},B)$:

$$\exists B \in [L (T_{hi}, B) > \text{PFM } (T_{hi})] \Rightarrow \text{Black hole node} \tag{4}$$

Lemma 2: In order to conduct a black hole attack, a black hole node increases sequence number and packet loss occurs.

Proof: Assume a black hole node increases its sequence number in RREP packet and advertise itself has having the highest sequence number in the network. The difference between the sequence numbers can be calculated by subtracting the sequence number send by current node from sequence number send by previous node in the network. Let us take SEQ_n be the value of sequence number of a node which can be calculated by:

$$SEQ_n = SEQ_c - SEQ_{c-1} \tag{5}$$

where, SEQ_c denotes the sequence number of current node and SEQ_{c-1} denotes the sequence number of previous node in the network. Let, $D (S_1,S_2)$ be a function that returns a difference between the sequence numbers between the hops. A route is subject to black hole attack if the difference $D (S_1,S_2)$ is max (SEQ_n). So:

$$\exists b \in \max (SEQ_n) > D (S_1,S_2) \Rightarrow \text{Black hole attack} \tag{6}$$

Theorem: The black hole attack can be detected by calculating lower layer feedback from MAC layer and upper layer feedback from network layer.

Proof: Let us assume lemma 1 and 2 are true. By lemma 1 packet forwarded at MAC layer can be calculated. By lemma 2, total number of missed sequence number can be calculated. By using this information the network load can be estimated. Therefore, if a node's MAC layer packet

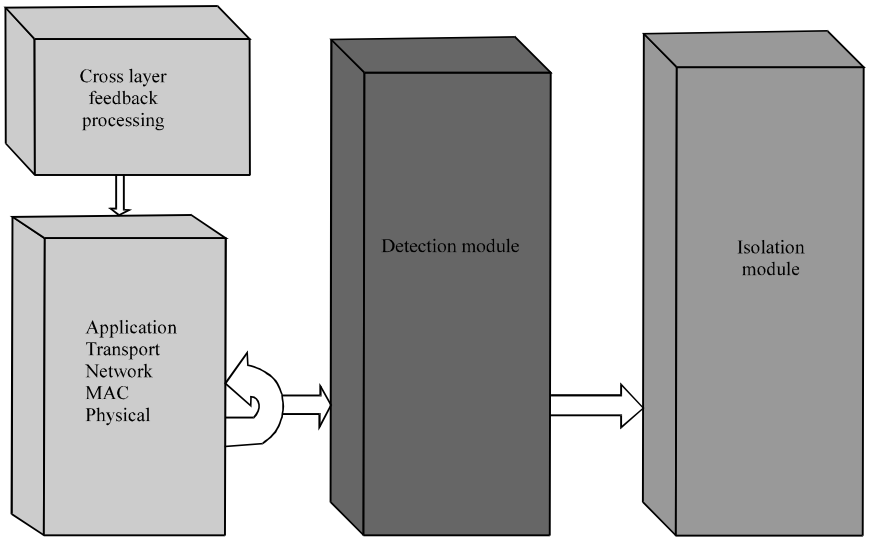

Fig. 1: Cross layer architecture

Table 1: Attributes used for cross layer architecture

Layer	Attributes
Network layer	IP sequence number
MAC layer	Packet loss

forwarded threshold is more or if difference between the sequence numbers is maximum then that node is concluded as black hole node. From Eq. 4 and 6:

$$\{\exists B \in [L(T_{hi}, B) > PFM(T_{hi})] \vee \exists b \in \max(SEQ_n) > D(S_1, S_2)\} \Rightarrow \text{Black hole node} \quad (7)$$

Cross layer architecture & cross layer algorithm: The proposed cross layer architecture is shown in Fig. 1. The principle elements are cross layer feedback processing module, detection module and isolation module.

Cross layer feedback processing: In cross layer feedback processing module we have created a feedback interface between MAC layer and network layer. Our new interface exposes internal information of MAC layer to the above network layer. This functionality is not previously accessible in traditional OSI layer. The following table illustrates the attributes used. As mentioned in Table 1 we have used the attributes of packet loss information from MAC layer. Whenever a black hole node interrupts the normal communication process it sends Fake RREP message to the source node. The fake RREP packet contains highest sequence number and lowest hop count information towards destination node. If a node is malicious that node forwards more number of same RREP message again and again to source node. When, the source node starts forwarding data, it forwards through this malicious black hole node. The black hole node drops this packet. This packet loss information is passed to above MAC layer. Additionally, the routing layer also calculated missed sequence number from routing layer which is a useful measure to calculate packet loss.

Table 2: Spoofed RREQ packet

Fields	Description
F1	Other fields in RREQ packets
DST	Nonexistence destination IP address
TTL	1

Detection technique: The proposed detection scheme includes the concept of RREQ spoofing to detect malicious nodes. In general packet spoofing is used by attacking nodes or malicious nodes in the network. The idea of spoofing is the spoofed packet is an Internet Protocol (IP) packet, created from a spoofed or fake IP address but it is impersonating to be a legitimate and authentic sender. Before discussing the proposed detection technique, now we explain about the important fields in AODV routing process. While in normal routing, when a node broadcast a RREQ, the TTL value is set up to a maximum value. Because the life time for the active route is updated until it reaches the destination node. Destination IP address is another field which is used to indicate the node to which a route is desired. During normal route discovery process a valid destination ID and a valid TTL is assigned for the nodes. But in our proposed detection technique, during communication process initially the black hole detector node sends spoofed RREQ packets (Table 2). The spoofed RREQ packet contains a nonexistent node ID and a TTL of 1. By receiving, this packet the black hole node replies that it

has the valid route to the particular node. So, this malicious node id is saved and isolated from other nodes.

Initially, the black hole detector initializes the malicious node detection process. First, it broadcast the spoofed RREQ packets (Table 2). Then this spoofed RREQ packet is broadcasted to all other nodes in the network. By using MAC layer and routing layer information, if any node reply to this spoofed RREQ packet that node is marked as black hole node. In this approach, we are using a timer which invokes the proposed detection process in some time interval. So, this approach uses dynamic detection of black hole attacks which uses the cross layer information. Then the black hole node is isolated from the network. The following pseudo code in algorithm A-D explains the proposed cross layer algorithm to detect black hole attack. The following pseudo code estimates the load caused by a potential black hole node.

Algorithm A: cross layer algorithm:

```
Function OnRecievingAODVPacket( )
Begin
//if the node is forwarding the same packet  again and again
 If  Total forwards  > CH_FORWARD_THRESHOLD {
        LowerLayerFeedback=true;
 }
//if the difference between the previous and present uid is big then it
signifies packet loss
if(SeqNumberMissig)
    {
      UpperLayerFeedback=true;
    }
if(LowerLayerFeedback || UpperLayerFeedback )
 {
 //Decreasing the variable     EstimatedAttackLoad will decrease the attack
detection timer interval
 EstimatedAttackLoad = EstimatedAttackLoad-LoadStep;
 } else {
 //increasing the variable     EstimatedAttackLoad will increase the attack
detection timer timer interval
 if (EstimatedAttackLoad <= LoadStep ) {
        EstimatedAttackLoad=LoadStep
else
 EstimatedAttackLoad=EstimatedAttackLoad + LoadStep;
}
//need not increase EstimatedAttackLoad beyond 1;
 if(EstimatedAttackLoad>MaxAllowedLoad) {
        EstimatedAttackLoad=MaxAllowedLoad
else
        EstimatedAttackLoad=EstimatedAttackLoad;
 }

Resume Normal AODV on receive  actions
……
……..
```

In the above pseudo code by combing MAC layer parameter and routing layer parameter we are checking for attack load in the network. After that the following pseudo code is important in order to find the black hole node. The following pseudo code is important in order to find the black hole node. The function recursively calls another function at periodic intervals. In the following function the timer is dynamically scheduled with respect to the previously estimated value of estimated attack load.

Algorithm B: the pseudo code of malicious node detection timer function:

```
Function MaliciousNodeDetectionTimer( )
Begin
  SendSpoofedRouteRequest();
  Interval ← MaliciousNodeDetectionInterval×EstimatedAttackLoad + Jitter
 //Schedule  next call to this function at Interval
  Schedule( MaliciousNodeDetectionTimer(),Interval )
End
```

The following pseudo code is responsible for sending spoofed route request which generates non existence node id.

Algorithm C: the pseudo code to send spoofed rreq request:

```
Function SendSpoofedRouteRequest()
Begin
    aodv_rt_entry *rt;
   //Create a non existing IP address
    NEAddress← NonExistingNodeID;
    rt ← rtable.rt_lookup(NEAddress);
    if(rt ==0) {
        rt ← rtable.rt_add(NEAddress);
    }
    SendFakeRequest(NEAddress);
End
```

The following function is the actual function which sends spoofed RREQ message by using send fake request method.

Algorithm D: the pseudo code for sending fake route request:

```
Function SendFakeRequest(NEAddress)
Begin
  // Allocate a RREQ packet
  SpoofedRREQ_Packet  Create_Default_RREQ_Packet()
  // Fill out the RREQ packet with Spoofed Info
  SpoofedRREQ_Packet->rq_TTL = 1;
  SpoofedRREQ_Packet->dst = NEAddress;
    Broadcast(SpoofedRREQ_Packet);
End
```

The following function modified route lookup function. While resolving a route AODV calls this modified route lookup function only. In side this function it finds next hop for a nonexistent node using the normal route lookup function. If there exists a nonexistent node in the routing table, then it signifies a nearby black hole node. If the next hop is a black hole then the algorithm just ignore it and search for the next possible next hop.

Isolation technique: After detecting the black hole nodes, now the information is updated in routing table which is discussed in algorithm E. By doing this we are marking that particular node as black hole node. So, the source node ignores the black hole node by not sending any packets through it. Thus, the black hole node is isolated from the network.

Algorithm E: the pseudo code for modified lookup:

```
Function On_Modified_Route_Lookup(Address)
Begin
   Detection Flag  ← false
  R1← Normal_ Route _Lookup(NonExistingNodeID);
  if (R1 &  R1->flags =RTF_UP ) {
    //there is a malicious node in the routing table
   Detection Flag ← true
   MaliciousNodeID ←  R1->Next hop;
   }
   for all route R in Routing Table do
     {
        // if the next hop of the returned route is via the
       // Non Existing Node then just ignore it
        if(Detection Flag & R->next hop =MaliciousNodeID)
        {
       //Next Hop is a Black Hold-Avoiding the route
           continue;
        }

        if(R->dst =id)  then      break;
       }
    return R;
End
```

RESULTS AND DISCUSSION

Experimental analysis: In this study, we evaluate the efficiency of the proposed technique against various network attributes. All the simulations are made on a Intel Core 2 DUO PC with 2 GB RAM. We used Cygwin with ns2.28. We have constructed the experimental networks for simulation purpose. The experiments are repeated with different parameters for MANET environment. During each run the trace files are saved and finally, the trace analysis is done to evaluate the performance. The following Table 3 illustrates the MANET working environment. Table 4 illustrates constant parameters for simulation. Table 5 illustrates variable parameters for simulation. The simulations are repeated for the following types:

- Type I; normal AODV
- Type II; AODV with Back Hole and without any detection
- Type III; AODV with back hole and with proposed dynamic cross layer based detection, with number of black holes 1-4

Table 3: The MANET environment

Property	Value	Description
Channel type	Wireless channel	Channel used
Propagation model	Two ray ground	The radio propagation model used
Antenna type	Omni antenna	Type of antenna
Interface queue type	Drop tail/priqueue	Queue used
MAC type	802.11	MAC layer protocol used
Maximum packets in queue	50	Packets in queue
Topological area	600×600 m	Area of simulation
Mobility scenario	10 m/s	Node's mobility
Pause time	20 sec	Node's pause time at simulation
Mobility model	Random way point	For mobility of nodes

Table 4: Constant parameter for simulation

Property	Values
Traffic agent	CBR
Transport agent	UDP
Traffic source	7
Traffic sink	7
CBR rate	10 Kbytes/s

Table 5: Variable parameter for simulation

Property	Values
Routing protocol	Normal AODV, AODV with black hole
No. of black holes	1-4
No. of nodes	20-60

For each type, we have repeated the simulation for 3 times and calculated the average of the results. For type II and III of experiment the simulations are run for 3×4 times (12 runs) with 20 normal nodes and 4 black hole nodes.

Performance metrics: List of four performance measurement parameters considered for this experiments are:

Packet Delivery Fraction (PDF): It is the ratio of CBR data packets received by all destinations (sinks) over the total number of packets sent by all the sources.

Normalized Routing Load (NRL): The normalized routing load is known as the ratio between control packets sent to that of receiving data packets.

End to End Delay (EED): End-to-end delay is the time taken for a packet to be transmitted across a network from source to destination

Overhead: The overhead is measured in terms of total generated routing packets. It is the count of total packet generated and forward at the network layer.

Total Dropped Packets: We count all the packets dropped due to any reason as a performance metric. In Table 6, we have tabulated the measured values of AODV protocol under normal condition.

Table 6: Type I; Analysis on normal AODV

PDF	NRL	EED	Routing packets	Dropped
97.60	0. 38	145.15	620.33	73

Table 7: Type II analysis on black hole AODV

Black hole nodes	PDF	NRL	EED	Routing packets	Dropped
1	67.73	0.45	68.24	493.33	590
2	44.13	0.72	49.17	430.00	983
3	26.87	1.01	42.34	445.67	1271
4	22.53	110.79	37.71	350.67	1350

Table 8: Type III proposed cross layer detection technique

Black hole nodes	PDF	NRL	EED	Overhead	Dropped
1	92.87	0.43	50.59	671.67	150
2	75.23	0.70	83.40	717.33	387
3	66.73	0.82	43.17	438.00	297
4	51.67	1.11	34.07	756.33	601

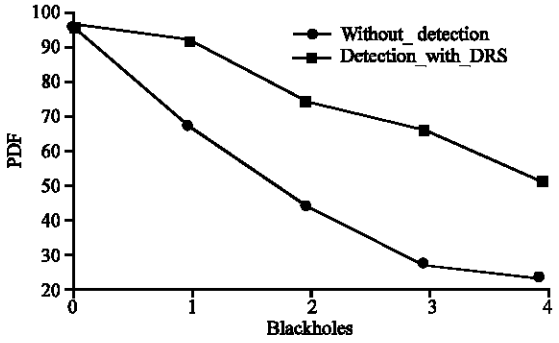

Fig. 2: PDF comparison graph

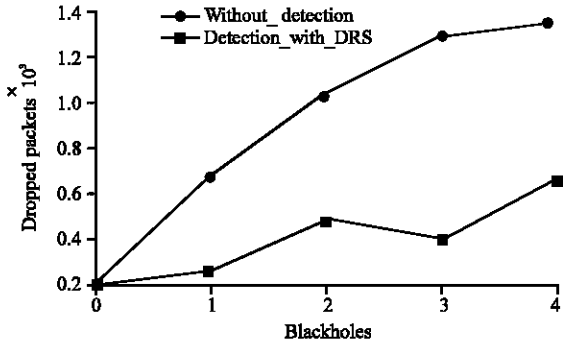

Fig. 3: Dropped packet comparison graph

In Table 7, we have tabulated all the measured values in the case of AODV protocol under black hole attack. Table 8 illustrates our proposed detection technique .While comparing Type II and III technique packet delivery ratio increases in our proposed thechnique. Packet drop ratio also greatly reduced. As shown in the following Fig. 2, in type II scenario packet delivery ratio gets decreased when increase in black hole nodes. But in proposed Type III technique, the cross packet delivery ratio is increased even though, there is the increase in the black hole nodes.

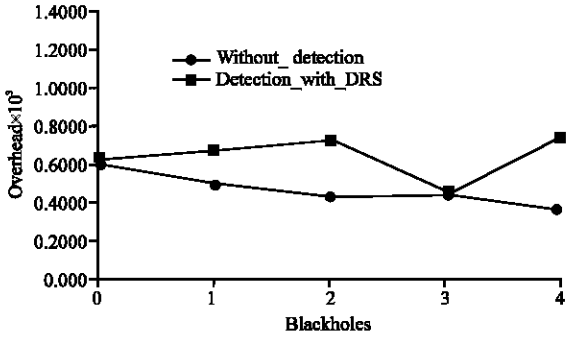

Fig. 4: Overhead comparison graph

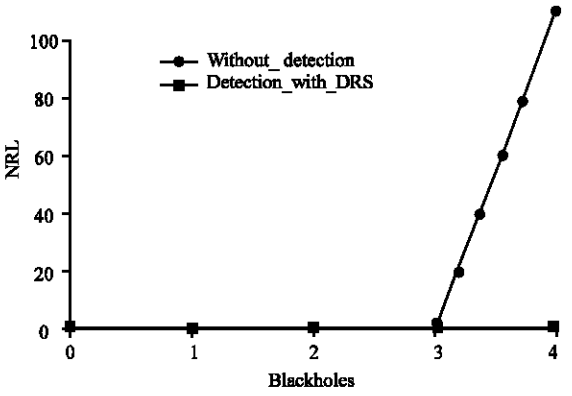

Fig. 5: Normalized routing load comparison graph

As shown in the following Fig. 3, the performance in terms of dropped packet is increasing with the increase of number of black holes in both cases. But, after detection and recovery, the dropped packet count is decreased considerably in type III technique. It means, the proposed method successfully detects black holes in the network and avoids forwarding packets through the black hole nodes.

In the following Fig. 4, we measured the overhead as the count of total generated and forward routing messages. As shown in Fig. 4, the performance of overhead is slightly decreased with the increase of black holes in type II technique. This is because the number of forwarded routing messages decreased due to the black hole since, a black hole try to consume all the packets instead of forwarding them. But with proposed Type III technique, the overall change in overhead is minimum. This is because, the extra messages used for black hole detection is very minimum and not consuming much network resources. As shown in the following Fig. 5, in the case of type I the Normalized Routing Load (NRL) is slightly increased with the increase of number of black holes. But, in proposed type III method, the normalized routing load is reduced.

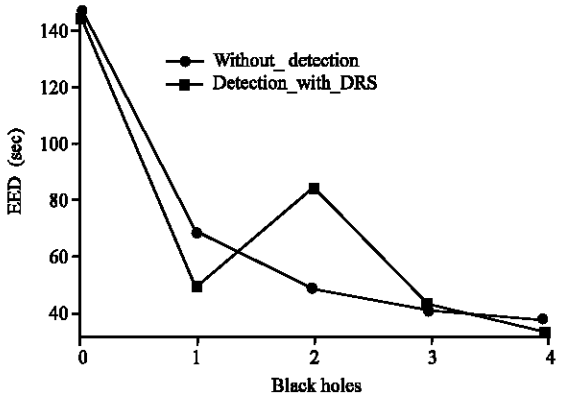

Fig. 6: End to End Delay (EED) comparison graph

Figure 6 shows the End to End Delay (EED). In Type III technique, the end-to-end delay is high for some time and then reduced. This is because after detection of black hole node, only the MANET consist of short path between source to destination. That is black holes affect all the lengthy paths and only the short path survive. So, the average of end to end delay is decreased with respect to the increase in black holes.

CONCLUSION

This study presents technique which uses dynamic cross layer approach. We have detected the black hole attack with various network conditions. We introduced the new interface between MAC layer to network layer in order to detect attacks efficiently. Packet delivery ratio increased in the proposed scheme. Packet drop ratio also decreased considerably. End to end delay is also decreased in the proposed approach. The detection process is called periodically and the routing table is updated dynamically. The proposed detection algorithm uses only a single spoofed RREQ message to detect the presence of black holes in the MANET environment. So, overhead also is greatly reduced in the network. Our future work focuses on considering different cross layer parameters to detect the black hole attacks in MANET.

REFERENCES

Al-Shurman, M., S.M. Yoo and S. Park, 2004. Black hole attack in mobile Ad Hoc networks. Proceedings of the 42nd Annual Southeast Regional Conference, April 2-3, 2004, Huntsville, AL. USA., pp: 96-97.

Burbank, J.L., P.F. Chimento, B.K. Haberman and W.T. Kasch, 2006. Key challenges of military tactical networking and the elusive promise of MANET technology. IEEE Commun. Mag., 44: 39-45.

Jaisankar, N., R. Saravanan and K.D. Swamy, 2010. A novel security approach for detecting black hole attack in MANET. Proceedings of the International Conference on Recent Trends in Business Administration and Information Processing, March 26-27, 2010, Thiruvananthapuram, India, pp: 217-223.

Joseph, J.F.C., A. Das, B.C. Seet and B.S. Lee, 2007. Cross layer versus single layer approaches for intrusion detection in MANETs. Proceedings of the 15th IEEE International Conference on Networks, November 19-21, 2007, Adelaide, SA., pp: 194-199.

Joseph, J.F.C., A. Das, B.C. Seet and B.S. Lee, 2008. CRADS: Integrated cross layer approach for detecting routing attacks in MANETs. Proceedings of the IEEE Wireless Communications and Networking Conference, March 31-April 3, 2008, Las Vegas, NV., USA., pp: 1525-1530.

Kannhavong, B., H. Nakayama, Y. Nemoto, N. Kato and A. Jamalipour, 2007. A survey of routing attacks in mobile Ad Hoc networks. IEEE Wireless Commun., 14: 85-91.

Lu, S., L. Li, K.Y. Lam and L. Jia, 2009. SAODV: A MANET routing protocol that can withstand black hole attack. Proceedings of the International Conference on Computational Intelligence and Security, Volume 2, December 11-14, 2009, Beijing, China, pp: 421-425.

Milanovic, N., M. Malek, A. Davidson and V. Milutinovic, 2004. Routing and security in mobile ad hoc networks. Computer, 37: 61-65.

Mistry, N., D.C. Jinwala and M. Zaveri, 2010. Improving AODV protocol against black hole attacks. Proceedings of the International MultiConference of Engineers and Computer Scientists, Volume 2, March 17-19, 2010, Hong Kong, pp: 1-6.

Nadeem, A. and M. Howarth, 2013. Protection of MANETs from a range of attacks using an intrusion detection and prevention system. Telecommun. Syst., 52: 2047-2058.

Pranusha, A. and G. Murali, 2015. A hybrid key management scheme for secure MANET communications. Int. J. Res. Eng. Technol., 4: 38-40.

Su, M.Y., 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comp. Commun., 34: 107-117.

Tamilselvan, L. and V. Sankaranarayanan, 2007. Prevention of blackhole attack in MANET. Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, August 27-30, 2007, Sydney, Australia, pp: 21.

Thamilarasu, G. and R. Sridhar, 2012. A cross-layer game for energy-efficient Jamming detection in ad hoc networks. Secur. Commun. Networks, 5: 364-373.

Yang, H., H. Luo, F. Ye, S. Lu and L. Zhang, 2004. Security in mobile ad hoc networks: Challenges and solutions. IEEE Wireless Commun., 11: 38-47.

Zhou, L. and Z.J. Haas, 1999. Securing Ad Hoc networks. IEEE Network, 13: 24-30.