International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume2, Issue 8 (August '2016)

PERFORMANCE EVALUATION OF BLACK HOLE ATTACK IN DSR USING IDS ALGORITHM: AN MISBEHAVIOR REPORT AUTHENTICATION

K.Ranjitha,
M.Phil Research Scholar,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Science College for Women (Autonomous),
Elayampalayam,Namakkal, Tamilnadu.

M.Jothilakshmi,
Assistant Professor,
Department of Computer Science and Applications,
Vivekanandha College of Arts and Science College for Women (Autonomous),
Elayampalayam,Namakkal, Tamilnadu.

Abstract: Mobile Ad hoc Network (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. The Proposed System is designed to resolve the weakness of Watchdog when it fails to detect misbehavior nodes with the presence of false misbehavior report. The core of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route. The proposed IDS algorithm maintains the list of all the nodes which send the route reply to the source with sequence number greater than the threshold value. The source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in When the RREQ message arrives to its final destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message. The performance of nodes transfer source to destination is high quality.

Keywords: MANET, MRA, IDS, RREQ.

I.INTRODUCTION

The migration to wireless network from wired network has been a global trend in the past few decades. The mobility and scalability brought by wireless network made it possible in many applications. Among all the coeval wireless networks, Mobile Ad hoc Network (MANET) is one of the most important and unique applications. On the contrary to traditional Network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages.

The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion detection mechanisms to protect MANET from attacks an intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, with the improvements of the technology and cut in hardware costs, we are witnessing a current trend of expanding MANETs into industrial applications. To adjust to such Trend, we strongly believe that it is vital to address its potential security issues.

II.METHODOLOGY

A) INTRUSION DETECTION SYSTEMS

Intrusion is any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource and an intrusion detection system (IDS) is a system for the detection of such intrusions. There are three main components of IDS: data collection, detection, and response. The data collection component is responsible for collection and pre-processing data tasks: transferring data to a common format, data storage and sending data to the detection module. IDS can use different data sources as inputs to the system: system logs, network packets, etc. In the detection component data is analyzed to detect intrusion attempts and indications of detected intrusions are sent to the response component.

In the literature, three intrusion detection techniques are used.It detects intrusions as anomalies, i.e. deviations from the normal behaviors. Various techniques have been applied for anomaly detection, e.g. statistical approaches and artificial intelligence techniques like data mining and neural networks. Defining normal behavior is a major challenge. Normal behavior can change over time and intrusion detection systems must be kept up to date. False positives – the normal activities which are detected as anomalies by IDS – can be high in anomaly-based detection. On the other hand, it is capable of detecting previously unknown attacks.

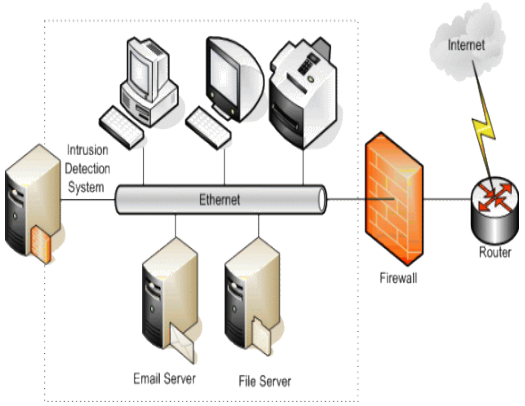

Figure 1: Black Hole Attack:

B) MISBEHAVIOR REPORT AUTHENTICATION

In this method we are avoiding false reports generated by the Misbehaving nodes. The main aim of MRA scheme is to authenticate whether the destination node has received the reported missing packet through a different route.

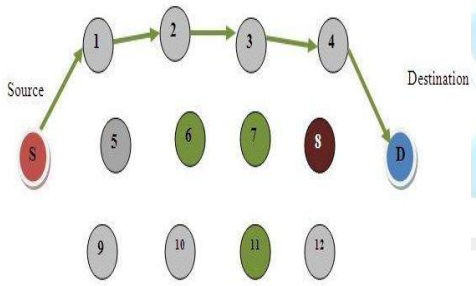

Figure 2: MRA Scheme authentications

In the above figure we can observe that between source and destination there are multiple paths available in MANET. So, to avoid false reports in secure ACK scheme we will find another path between source and destination and source will check the reports which it gotten from intermediate nodes if any false report found means it will treat the node which sent that report as a misbehaving node.

C) USING IDS ALGORITHM:

The source waits for the destination to send acknowledgement to it after every 10th packet. If source receives the acknowledgement, then there is no misbehaviour in the network and process continues as such. But if the destination fails to acknowledge the data packets for a time period, then IDS starts its functionality. As in black-hole attack, there is a greater possibility that black-hole node will send the highest sequence number to the source in route reply. The proposed IDS algorithm maintains the list of all the nodes which send the route reply to the source with sequence number greater than the threshold value.

The IDS will be applied only on those nodes which are in the list maintained by ids.

Algorithm 1: Algorithm for detecting IDS

Input: Threshold_seq_no. Set_of_all_nodes; Set_of_nodes_who_sent_route_reply; source; destination;

1. Begin
2.If(pkt_received_by_dest==pkt_sent_by_source) then
3. Network does not shows any malicious behaviour
4. Else if (pkt_received_by_dest < certain percentage of pkt sent by source over the
   network)
5. {
6. Then the network shows malicious behaviour and IDS is applied to detect malicious behaviour
7.For(inti=0;i<no._of_nodes_who_sent_route_reply;
   i++)
8. {
9.If(seq_no[route_reply[Node]]> Threshold_seq_no) then
10. List. add(next[Node])
11. List. add(Node)
12. List. add(prev[Node])
13. result= Segment_watchdog(List);
14. If(result==true) then //(i.e. if malicious node is found)
15. Exit;
16. ENDIF
17. Else
18. Continue
19. Endelse
20. }
21. }

Algorithm: Segmented Watchdog (List)

The watchdog method detects misbehaving nodes. Figure 2 illustrates how the watchdog works. Suppose there exists a path from node S to D through intermediate nodes A, B, and C. Node A cannotransmit all the way to node C, but it can listen in on node B's traffic. Thus, when A transmits a packet for B to forward to C, A can often tell if B transmits the packet. If encryption is not performed separately for each link, which can be expensive, then A can also tell if B has tampered with the payload or the header. The watchdog technique has advantages and weaknesses. DSR with the watchdog has the advantage that it can detect misbehavior at the forwarding level and not just the link level. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior, 5) collusion, and 6) partial dropping. If a packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds acertain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node.

1. BEGIN
2. Result=false

3. malicious= Null
4. Node1= list. get(0)
5. Node2= list. get(1)
6. Node3=list. get(2)
7. //Chk(Sent_pkt[Node2]);
8. If(sent_pkt[Node2] == Received_pkt_by_node2) THEN
9. Monitor Node3
10. ENDIF
11.If(Sent_pkt_by_Node3==Received_pkt_by_Node3) THEN
12. No malicious activity detected in this segment
13. RETURN Result
14. END IF
15.Elseif(Sent_pkt_by_Node1< Received_pkt_by_Node1) THEN
16. Malicious= Node1
17. Result= True
18. RETURN Result
19. END ELSEIF
20.Elseif(Sent_pkt_by_Node2< Received_pkt_by_Node2) THEN
21. Malicious= Node2
22. Result=True
23. RETURN Result
24. END ELSEIF
25.Elseif(Sent_pkt_by_Node1< Received_pkt_by_Node1) THEN
26. Malicious= Node1
27. Result=True
28. RETURN Result
29. END ELSEIF
30. END

III. DESCRIPTION OF BLACKHOLE ATTACK

In AODV, Dst Seq (destination sequence number) is used to determine the freshness of routing information contained in the message from originating node. When generating a RREP message, a destination node compares its current sequence number, and Dst Seq in the RREQ packet plus one, and then selects the larger one as RREP's Dst Seq. Upon receiving a number of RREP, a source node selects the one with greatest Dst Seq in order to construct a route. To succeed in the blackhole attack the attacker must generate its RREP with Dst Seq greater than the Dst Seq of the destination node. It is possible for the attacker to find out Dst Seq of the destination node from the RREQ packet. In general, the attacker can set the value of its RREP's Dst Seq base on the received RREQ's Dst Seq. However, this RREQ's Dst Seq may not present the current Dst Seq of the destination node. Figure 3 shows an example of the blackhole attack. The value of RREQ and RREP using in the attack are shown in Table 1

	RREQ		RREP		
	a1	b1	c1	d1	e1
IP.Src	S	A	D	A	D(MD)
AODV.Dst	D		D		D(DM)
Dst Seq	60		61		65
AODV.Src	S		-		-

Table 1: Values of RREQ and RREP

In Table 1, IP.Src indicates the node which generate or forward a RREQ or RREP, AODV.Dst indicates the destination node and AODV.Src indicates the source node. Here, we assume that the destination node D has no connections with other nodes. The source node S constructs a route in order to communicate with destination node D. Let the destination node D's Dst Seq that the source node S has is 60. Hence, source node S sets its RREQ(a1) and broadcasts as shown in Table 1. Upon receiving RREQ(a1), node A forwards RREQ(b1) since it is not the destination node. To impersonate the destination node, the attacker M sends spoofed RREP(e1) shown in Table 1 with IP.Src, AODV.Dst the same with D and increased Dst Seq (in this case 65 as) to source node S. At the same time, the destination node D which received RREQ(b1) sends RREP(c1) with Dst Seq incremented by one to node S. Although, the source node S receive two RREP, base on Dst Seq the RREP(e1) from the attacker M is judged to be the most recent routing information and the route to node M is established. As a result, the traffic from the source node to the destination node is deprived by node M.

VI. NETWORK SIMULATOR (NS2)

NS-2 is a packet-level simulator and essentially a centric discrete event scheduler to schedule the events such as packet and timer expiration. Centric event scheduler cannot accurately emulate "events handled at the same time" in real world, that is, events are handled one by one. This is not a serious problem in most network simulations, because the events here are often transitory. CMU Monarch Project, has 2 assumptions simplifying the physical world. Nodes do not move significantly over the length of time they transmit or receive a packet. This assumption holds only for mobile nodes of high-rate and low-speed.

For simulation, we set the parameter as shown in Table 2. Random Waypoint Model (RWP) is used as the mobility model of each node. In this model, each node chooses a random destination within the simulation area and a node moves to this destination with a random velocity

Simulator	ns-2(ver.2.27)
Simulation time	600(s)
Number of mobile nodes	30
Topology	1000m × 1000m
Transmission Range	250m
Routing Protocol	AODV
Maximum Bandwidth	2Mbps
Traffic	Constant bit rate
Maximum Speed	5(m/s)
pause time	10(s)

Table 2: Simulation parameters

Here, we assume that the blackhole attack take place after

the attacking node received RREQ for the destination node that it is going to impersonate.

V. PERFOMANCE EVALUATION:

MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly. Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry. However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes and presumably not malicious attackers can easily compromise MANETs by inserting malicious or non cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system (IDS) specially designed for MANETs.

VI. FUTURE ENHANCEMENT

Furthermore, in an effort to prevent the attackers from initiating a forged acknowledgement attacks, extended to incorporate digital signature in proposed scheme. Although it generates more routing overhead in some cases, as demonstrated in experiment, it can vastly improve the networks packet delivery ratio when the attackers are smart enough to forget acknowledgement packets. This trade-off is worthwhile when network security is of top priority. In order to seek the optimal digital signature algorithms in MANETs, implemented both DSA and RSA scheme in our simulation.

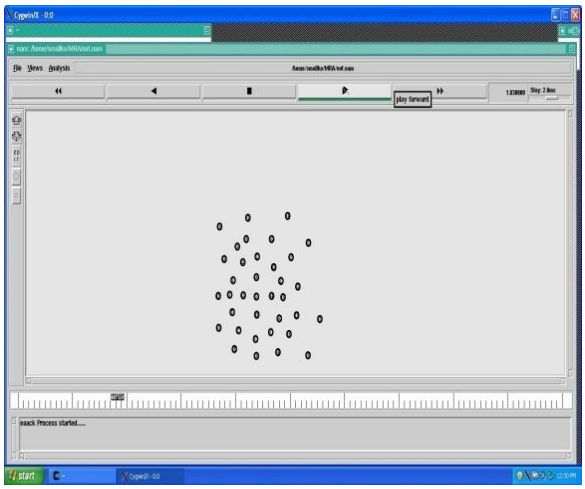

Figure 3: Creation of Node

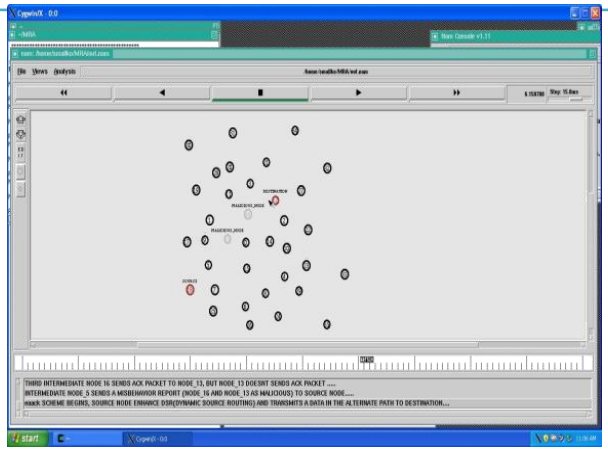

Figure 4: MRA Scheme

Figure 5: Routing Overhead Scenario

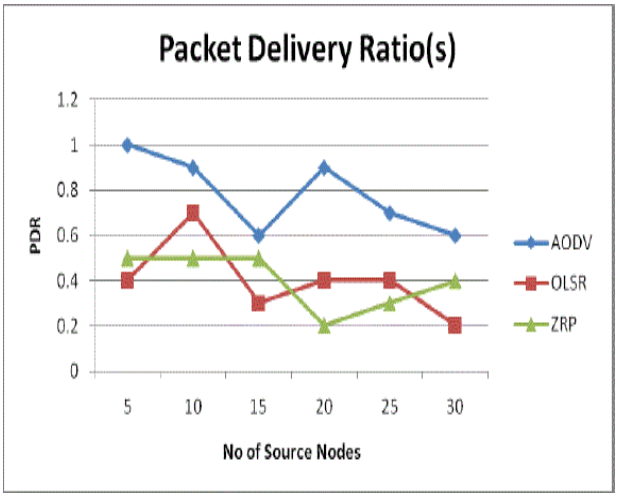

Figure 6: Performance Evaluation

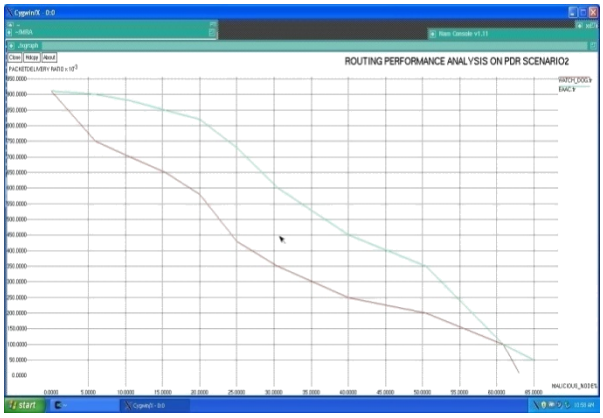

Figure 7: Packet Delivery Ratio

VII. CONCLUSION

In this paper, we proposed a neighbor set based approach to detect black hole attack and **a** muting recovery protocol to mitigate the effect of black bole attacks. The IDS algorithm maintains the list of all the nodes which send the route reply to the source with sequence number greater than the threshold value. We demonstrated through simulation that our methods could effectively and efficiently detect black hole. in an effort to prevent the attackers from initiating a forged acknowledgement attacks, extended to incorporate digital signature in proposed scheme. Although it generates more routing overhead in some cases, as demonstrated in experiment, it can vastly improve the networks packet delivery ratio when the attackers are smart enough to forget acknowledgement packets. This trade-off is worthwhile when network security is of top priority. Identifying a malicious node in a network has been a reoccurring challenge

REFERENCES

[1]. Alomair,B. and Poovendran,R.(2010) "Privacy versus Scalability in Radio Frequency Identification Systems," Computer Comm., vol. 33, no. 18, pp. 2155-2163.

[2]. Alomair,B. Clark,J. Cuellar,J. and Poovendran,R.(2010) "Scalable RFID Systems: A Privacy-Preserving Protocol with Constant-Time Identification," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 8, pp. 1536-1550.

[3]. Bogdanov,A. Knudsen,L. Leander,G. Paar,C. Poschmann,A. Robshaw,M. Seurin,Y. and Vikkelsoe,C.(2009) "PRESENT: AnUltra-Lightweight Block Cipher," Proc. Workshop Cryptographic Hardware and Embedded Systems (CHES '07), pp. 450-466.

[4]. Bogdanov,A. Leander,G. Paar,C. Poschmann,A. Robshaw,M. and Seurin,Y.(2008)"Hash Functions and RFID Tags: Mind the Gap," Proc. 10th Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '08), pp. 283-299.

[5]. Feldhofer,M. Dominikus,M. and Wolkerstorfer,J.(2004) "Strong Authentication for RFID Systems Using the AES Algorithm," Proc.

[6]. C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," IEEE Transactions on Mobile Computing, vol. 2, no. 3, pp. 257-269, Jul./Sep. 2003.

[7]. H. Deng, W. Li, and D. P. Agrawal, "Routing security in ad hoc networks," IEEE Communications Magazine, vol. 40, no. 10, pp. 70-75, Oct. 2002.

[8]. Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," in Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pp. 12-23, Sept. 2002.

[9]. Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Crossfeature analysis for detecting ad-hoc routing anomalies," in The 23rd International Conference on Dis- tributed Computing Systems (ICDCS'03), pp. 478- 487, May 2003.

[10]. A. Baadache, and A.Belmehdi, "Avoiding Black hole and Cooperative Black hole Attacks in Wireless Ad hoc Networks," International Journalof Computer Science and Information Security," Vol. 7, No. 1, 2010.

[11]. V. K and A. J PAUL, "Detection and Removal of CooperativeBlack/Gray hole attack in Mobile Ad Hoc Networks," 2010 InternationalJournal of Computer Applications, Vol. 1, No.22, 2010

[12]. Evans, R.G. Yunseop Kim and W.M. Iversen, "Remote Sensing and Control of an Irrigation System Using a Distributed Wireless Sensor Network," *IEEE*, vol. 57, no. 7, pp. 1379 - 1387, May 2008.

[13]. Jin-Shyan Lee and Hsinchu Ind. Technol. Res. Inst., "A Petri Net Design of Command Filters for Semiautonomous Mobile Sensor Networks," *IEEE*, vol. 55, no. 4, pp. 1835 - 1841, April 2008.

