RESEARCH REVIEW JOURNALS
Volume-02
Issue-12
December-2017

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com

IAACK- Intrusion Detection System for MANETs

*[1]A. Priyadharshini & [2]A. Sekar

*[1]Assistant Prof., Dept of Information Science and Engineering, CMR Institute of Technology, Bangalore, Karnataka (India)
[2]Assistant Prof., Dept of Computer Science and Engineering, Knowledge Institute of Technology, Salem, Tamil Nadu (India)

ARTICLE DETAILS

Article History

Published Online: 29 December 2017

Keywords
MANETs, Black Hole attack, OLSR

***Corresponding Author**
Email: priyacse.6@gmail.com

ABSTRACT

MANET - Mobile Adhoc Networks are type of wireless networks that doesn't need any infrastructure. In MANET, the position of the nodes will change dynamically. At any point of time, any node can enter and leave the network. Every node in the network acts as a router. MANET is widely used in military applications. As there is no centralized administration an attacker can easily launch an attack in the type of network. There are varieties of attacks that can be launched in MANET. Among that Black hole attack causes more deviating damage. This paper deals with co-operative black hole attack which is more severe than black hole attack. In the paper, we have proposed an approach that uses OLSR.

INTRODUCTION

Ad-hoc network is a type of wireless rule that doesn't have centralized administration. There are 2types of Ad-hoc network. 1. Static 2. Mobile, in static ad-hoc network the position of the nodes is fixed. In mobile ad-hoc network the position of the nodes will change dynamically limited battery power, lower bandwidth, dynamic topology, security are some of the constraints in MANET. In MANET, at any time any node can enter and leave the network. Each nodes act as a router i.e., each node as the capacity to send and receive packets. MANET's are widely used in Military applications, conference halls and in places where traditional network is difficult to deploy.

Due to its dynamic topology, it is bare to variety of attacks. Among them black hole attack causes more deviating damage to MANET. Black hole attack is a type of denial of service attack. In denial of all service attack, the attack will flood the target node either with route request or by messages. So that the target node will be overloaded and it won't serve the legitimate nodes, i.e., the service provided by the target node is disrupted. In black hole attack the attacker node will send fake route reply to the route request. A fake route will be formed via the attack node. The attacker will modify /delete/delay the packets that are passing through it.

In cooperative black hole attack the attackers will join together and launch attack like black hole attacks. Cooperative black hole attack is very severe and it is very difficult to detect and to prevent. Lot of research is going to overcome cooperative black hole attack.

AODV protocol is used in [1], which is efficiency in dealing with multiple black hole attack. But, in AODV, every time routing request process need to be carried out. In order to overcome that Zone Routing Protocol is used.

MANET routing protocol have been classified into three categories.

- Reactive routing protocol
- Protective routing protocol
- Hybrid routing protocol

Routing process: routing is the process of finding the optional route to the destination. In the MANET routing process is carried out in four stages. 1. Route advertisement (RA), 2. Route request (RRQ), 3. Route reply (RRP), 4. Route error (RE).When the node enters the network the node send a RA to its route. If a node enters to the send data then it need to establish route to the destination. So the sender node populate route regarding path to the network. If a route exists then the node will send route reply message to the source node.

As the network is dynamic any node can leave the network any time. If a node leaves then the network intermediate node will send the route error message to the source node.

Proactive: Once the route has been establishment remains valid until the node moves from the network. E.g: Optimized Link State Routing Protocol, Destination Sequenced Distance Vector Routing Protocol

Reactive: the route will be established only when the route data send and once the data has been transmitted the route will be inactive (deleted). Advantage less network overhead and the disadvantage is high processing overhead. E.g.: Adhoc On demand, Dynamic Source Routing Protocol. Hybrid: It combines both proactive and reactive routing protocols.

E.g.: Zone Routing Protocol

In existing enhanced AODV protocol DRI table is maintained.

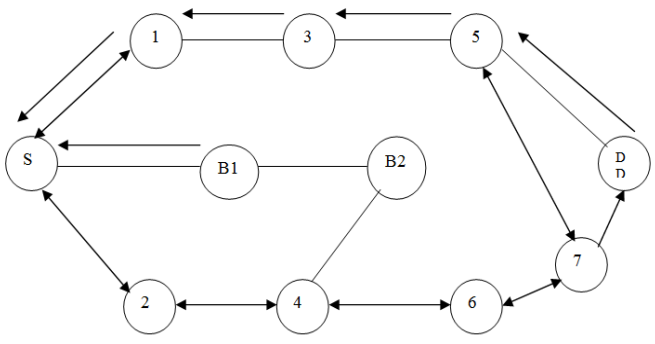

Fig.1. Detection of cooperative black hole attack

Table-1DRI Routing Table maintained by node 4

Nodes	Data routing interface	
	From	Through
5	1	0
6	1	1
B2	0	0
2	1	1

Fields in DRI routing Table:

Data routed from and routed through to nodes maintained by the node n. Node n has routed data packets from node 5, but has not routes any data packets through 5 (before node 5 moved away from node 4) both from 1 & through 1.

Reactive link verification

In dynamic network reactive link verification is difficult. Reactive link verification is best suited for reactive routing protocols. In proactive method, a cache of recently verified neighbours is maintained, with an expiry internal (temp). Nodes using this method perform no link verification until the use of a link is needed.

A node waits until it receives a broadcast packet across a previously unverified link during the reactive link verification process for a broadcast route request. At this time, it initiates a link verification exchange with the sender of the packet. To avoid a potential "implosion" effect, where many receives try to initiate an exchange at the same time, the receiver waits for a small randomly selected time internal before initiating the link verification exchange.

During the time internal enquiry internal, a node may believe that it has a link with a neighbor, when infant the neighbor has moved away. A window of opportunity for a black hole attack faking the previously existing link is provided. Thus the value of expiry internal provides a trade-off between high overload due to frequent verification and attack vulnerability due to potentially absolute information.

MATHEMATICAL MODEL

STAGE1: Detection of single black hole node.

In Fig. 1, the path is selected as S-B1-B2-4-6-7-D.

N- Number of node in the link, n→ Number of packets that have been send by the source. μ-threshold problem of packet drop rate due to network issues

Consider the route S-B1-B2-4

When node B1 responds to source node S with RREP message, it provides its next hop node B2&DRI for the next hop. (if B1has routed data packets through B2). Here the black hole node lies about using the path by replying with the DRI value to 01. Upon receiving RREP message from B1, the source node S will check its own DR1 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. Therefore S sends further request to B2 via alternate path S-5-6-B2 & asks B2 about 3 things.

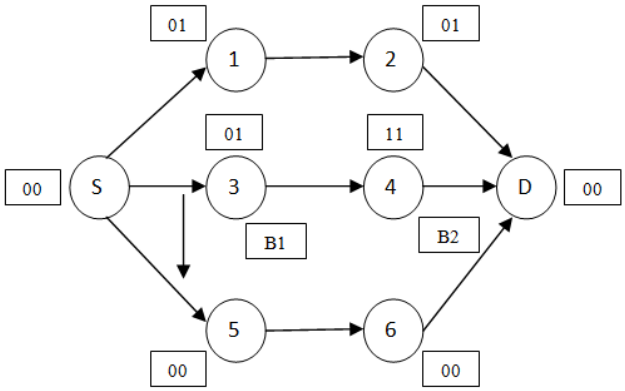

Fig. 2 Detection of cooperative black hole attack by using DRI table

If B2 has routed any data from B1, who is B2's next hop & if B2 has routed data packets through B2's next hop. Since B2 is collaborating with B1, it replies positively to all the 3 requests & gives node 6 (randomly) as its next hop.
The S rechecks with 6→reply negative.

DR1 table B2 0 0.

S consider B2 as black hole node, since B1 need to check (validate) before sending data through B2. Hence B1&B2 are marked as attackers.

Link verification→2 nonce & signature (ECC signature). This rendezvous phase is implemented as a single RTS-CTS DATA-Ack exchange.

Step 1→request to send (R) : Initiator, i sends an RTS to j.
Step2→ CTS(Clear to Send) (αj): After Short Interframe Space (SIFS) – Small time interval between the data frame and its ack [CTS + αj]
Data(βi)-> Data+header(nonce)-> rendezvous packet[Data+ βi]
Ack <- Ack pair(αj, βi)
According to Binomial theory[5], packets received at next hop node (NHN) of source= n(1-μ)
Packet received at next to NHN of source= n(1-μ)(1-μ)=n(1-μ)^2 for Nth node, ū= n(1- μ)^N
Assume n=100 μ=0.08 9 (i.e., 8 packets may be dropped in normal state)
Calculation at B1
Where n=100
μ=0.08
N=1 (i.e., first node)
$\bar{u}_1$=100(1-0.08)^1= 100(1-0.08)=92
for B2 N=2 (2nd node)
$\bar{u}_2$=84 for node 4. N=3 (i.e., 3rd node)
$\bar{u}_3$=76.

Table II: Scenario for Mathematical Model

Nodes	S	B1	B2	4
Without black hole	100	92	84	76
With black hole	100	92	0	0

B1 is malicious hence it will drop all the incoming packets from the source S. So ū2 and all ūN will be 0. Here B1 is

black hole node and hence next node i.e., B2 is checked for black hole attack.

CONCLUSION

Co-operative black hole attack which is more severe than black hole attack has been proposed. To overcome the vulnerabilities of AODV protocol OLSR protocol is used. True-Link-crosschecking method is designed to isolate and mitigate the effect of black hole attacks on MANET. True-Link-crosschecking enhances AODV protocol to improve the network performance by improving routing update condition. This solution reduces routing overhead and delay. It achieves maximum throughput when number of nodes and pause time more. In future work, we are planning to reduce routing overhead by making nonce more secure and timestamp in link verification.

REFERENCES

[1] R. Prasad, S. Dixit, R. Van Nee, "Globalization of mobile and wireless communication" in , pp. 335, March 2011, Springer.

[2] L. Gavrilovska, R. Prasad, "Ad hoc Networking towards seamless communications" in , pp. 284, 2006, Springer.

[3] J. Sen, S. Koilakonda, A. Ukil, "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks", Second international conference on intelligent system modeling and simulation, pp. 25-27, 2011.

[4] L. Tamilselvan, V Sankar Narayana, "Prevention of black hole attack in MANET", Journal of Networks, vol. 3, no. 5, pp. 13-20, 2008.

[5] S. Banerjee, "Detection/Removal of cooperative black and gray hole attack in mobile ad-hoc networks", *The World Congress on Engineering and Computer Science*, 2008.

[6] J. Eriksson, S. V. Krishnamurthy, M. Faloutsos, "TrueLink: A practical countermeasure to the wormhole attack in wireless networks", The Communications and Networks Consortium sponsored by the U. S. Army Research Laboratory under the Collaborative Technology Alliance Program., 2011.

[7] H. Weerasinghe, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, vol. 2, pp. 362-367, 2007.

[8] C. Perkins, E. B. Royer, S. Das, "Ad hoc On Demand Distance Vector (AODV) Routing Internet Draft", RFC 3561 IETF Network Working Group, July 2003.

[9] C. Wu Yu, W. Tung-Kuang, ReiHeng Cheng, S. Chao Chang, "A distributed and cooperative black hole node detection and elimination mechanism for ad hoc networks", PAKDD International Workshop Nanjing, pp. 538-549, 2007.

[10] C. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector Routing", *Proceeding of the* 2nd IEEE Workshops on Mobile Computing System and Applications (WMCSA), pp. 90-100, Feb. 1999.

[11] G. D. Wahane, A. M. Kanthe, D. Simunic, "Technique for detection of cooperative black hole attack using true link in mobile adhoc networks", MIPRO 2014 IEEE Conference.

[12] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks, In Proceedings of the 8thInternational Conference on Mobile Computing and Networking(Mobicm 2002), pp. 12-23, ACM, Atlanta, GA, Sept 2002.

