IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Detection and Prevention of Wormholl Attack Using AODV Protocol

Miss Asha Mansore[1], Miss Surbhi Koushik [2]

M. Tech DC PCST College, Indore[1]

Asst. Professor Electronics Department, PCST College, Indore[2]

Abstract: Due to wireless communication in Mobile Ad hoc Network (MANET) it is vulnerable to different routing attacks. One of the severe network layer attacks is wormhole attack, which totally disrupts the channel without disturbing the traditional routing protocol. In this paper, we have discussed about wormhole attack, its behavior and technique of its deployment, detection and prevention available currently. At last we suggested a cluster-based energy-efficient method to detect and prevent malicious node in the cluster.

Keyword: MANET, AODV, WSN, Wormhole, Cluster-based.

1. INTRODUCTION

In recent years, in the field of wireless communication and networking considerable advancements have been experienced. MANETs have become very popular. Ad hoc is derived from Latin, meaning "for this purpose" meaning temporary. "Mobile Ad hoc Networks" as the name reflects is a temporary deployed mobile wireless network. Ad hoc networks by their features help to address some issues relating connectivity between two devices. With the evolution of Internet data communication or networking between two devices came into existence. But because of the way the Internet is structured two devices that are in immediate wireless range of each other still have to use routers and switches at remote locations to forward packets between each other. Ad hoc networks are able to change this by directly connecting multiple wireless devices without the aid of any infrastructure. Usually ad hoc networks are created on-the-fly for a particular one-time purpose. Here, each node in the network acts as a host as well as a router and performs network control operations. Therefore, these networks are quick and easy to deploy, unlike infrastructure-based networks. Because of these characteristics ad hoc networks are becoming popular for applications such as: conferencing, emergency services for military and disaster management, sensor networking, and intelligent transportation systems. Ad hoc networks may also be used in campuses, companies and hospitals for connecting devices that are nearby.

MANET is a multi-hop, temporary, self-organizing system made up of a group of portable electronic equipments with wireless transmitter and receiver. This collection of mobile nodes may operate in isolation, or may have gateways to interface with a fixed network. An ad-hoc network uses no centralized administration.

Nodes in MANET are equipped with portable communication devices. These nodes may vary in size and capabilities. They could be small sensors with very limited computation, communication, and energy capabilities. Or there may be larger more powerful nodes such as laptops or even vehicles that are equipped with communication and computation devices. In MANETs nodes may be deployed in large numbers and can typically have a large span. The nodes could be distributed in the network either randomly or in a fixed grid.

In mobile ad hoc networks, communication is established via peer-to-peer links between individual pairs of nodes. If a mobile node is within the transmission range of another node, they can communicate with each other directly. Because of the limited transmission range of the nodes, multiple hops may be needed to reach other nodes. Every node connected to an ad-hoc network must forward packets for other nodes also. Intermediate nodes which fall in communication range of host nodes must act as router and enable communication between farther nodes. Thus nodes must communicate and cooperate with one another to forward data packets to their final destinations. Thus every node acts both as a host and as a router. A mobile host is simply an IP-addressable host or entity. A router is an entity, which is able to run a routing protocol. Thus nodes in the ad hoc network perform routing function to help each other in relaying packets and construct a network themselves.

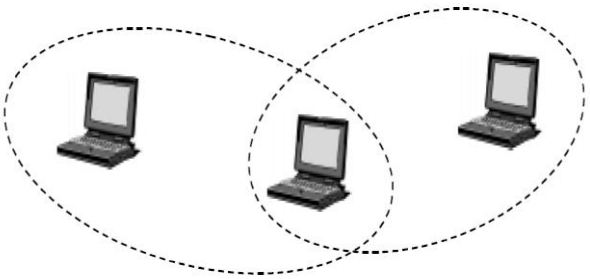


Figure 1 .Example of a simple ad-hoc network with three participating nodes.

Figure 1 shows a simple ad-hoc network. Three nodes are shown with the communication range. The outer nodes are not within transmission range of each other. However the middle node can be used to forward packets between the

outer nodes. Thus the middle node is acting as a router and the three nodes are forming an ad-hoc network.
MANETs are different from other ad-hoc networks because of rapidly changing network topologies. If one of the mobile nodes moves out of transmission range of the others the network doesn't collapse. Nodes are able to join and leave the network whenever they want i.e. nodes are free to move randomly and in any direction. As the nodes move dynamically, keeping track of the network topology is a difficult task. This topology information must be updated periodically as the routes change dynamically. Ad-hoc networks are capable of handling these topology changes and malfunctions in nodes. For instance, if a node leaves the network and causes link breakages, affected nodes can request for new routes and the network can be reconfigured. This requires use of packet-routing algorithms in which the nodes maintain the route information.

2. AD-HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOLS (AODV)

AODV is a reactive routing protocol designed for ad hoc wireless networks. In AODV routes to connect two nodes are obtained only when it is required i.e. on demand. AODV routing algorithm is specially suited for dynamic self-configured networks like MANET. AODV provides loop free routes along with route management for broken links. Bandwidth requirement of mobile nodes in AODV is comparatively less than other protocols as AODV does not require periodic route advertisements.
There are three types of control messages in AODV which are discussed below.

Route Request Message (RREQ):
Source node that needs to communicate with another node in the network transmits RREQ message. AODV floods RREQ message, using expanding ring technique. There is a time to live (TTL) value in every RREQ message, the value of TTL states the number of hops the RREQ should be transmitted.

Route Reply Message (RREP):
A node having a requested identity or any intermediate node that has a route to the requested node generates a route reply RREP message back to the originator node.

Route Error Message (RERR):
Every node in the network keeps monitoring the link status to its neighbour's nodes during active routes. When the node detects a link crack in an active route, (RERR) message is generated by the node in order to notify other nodes that the link is down.

3. LIMITATION OF CURRENT SYSTEM

A malicious node can carry out the following attacks in AODV.
1. Source node can be impersonated by the malicious node by modifying the source address with its address in the RREQ packet.
2. To analyze the communication in the route and become a part of it, malicious node can change the other contents of RREQ packet also such as hop count. It reduces the hop count in order to increase the chances of being selected in the route between source and destination.
3. Destination node can also be impersonated by forging the destination address by its own address in a RREP.
4. Malicious node can capture an entire network and act as a network leader by broadcasting the biggest sequence number. It can become a black hole to the entire sub network.
5. It can selectively forward certain RREQ packets and RREP packets and avoid other packets.
6. It can forge a RERR message and avoid further communication between nodes as they cannot reach the destination with different sequence number.
7. To create delay in the communication, malicious node can send two different RREQs to the neighboring node with different sequence numbers.

4. WORMHOLE ATTACK

A Wormhole attack is used to compromise the network by capturing or introducing better communication node then existing sensor nodes to degrade the performance. There are five methods to apply wormhole attack on AODV. The attacker uses high power transmission node or high bandwidth tunnel to create illusion of shortest path among nodes. Attacker uses these quality techniques to promote itself for route discovery or data packet communication. Due to quality shortest route, neighbor gets wonder and adopt the solution for communication. Once connection establish, attacker collect data packet one end and deactivate the forwarding link

A typical wormhole attack requires two or more attackers (malicious nodes) having better communication capability and resources than other sensor nodes. The attacker creates a low-latency link (high-bandwidth tunnel) between two or more attackers in the network. Attackers promote these tunnels as high-quality routes to the base station. Hence, neighboring sensor nodes take up this tunnel for their communication. The strange factor is, all data packet moves from this tunnel and attacker may collect or drop data packet respectively.
Following wormhole technique may be used to implement wormhole attack in MANET.

- Wormhole Using Encapsulation
- Wormhole Using High-quality/Out-of-band Channel
- Wormhole Using High-power Transmission
- Wormhole Using Protocol Distortion.
- Wormhole Using Packet Relay

5. PROBLEM DOMAIN

The major security issue with ad-hoc network is insecure routing. Even though, a large amount of work has been done in this area but all the proposed techniques are based on stationary strategies. They do not consist of current network traffic, security factor of midway nodes and selected route. Further, the susceptibility of routing process gives opening to attackers for compromising sensor nodes or intermediate messages to misguide routing

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

process or bring network into endless state. One of the major draw backs of insecure routing is increased routing time, unnecessary energy utilization, resource consumption and restricted access conditions during communication.

Ad-hoc network are vulnerable to various types of attacks. These attacks are mainly: Attacks on secrecy and authentication (outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets), Attacks on network availability (attacks on availability of Ad-hoc network are often referred to as denial-of-service (DoS) attacks), Stealthy attack against service integrity (the goal of the attacker is to make the network accept a false data value).

6. PROPOSED TECHNIQUES (HOP COUNT ANALYSIS APPROACH)

This research work proposes an efficient technique to detect and prevent wormhole attack without the need for special hardware or strict location or synchronization requirements. The proposed technique makes use of variance in routing information between neighbors' to detect wormholes. The detection technique uses an approach based on hop count. The wormhole affected routes are distinguished from legitimate routes by analyzing the hop count value of all paths. The basic idea of the technique is to discover alternative routes to the destination. These alternative routes will be extensively dissimilar in length i.e. the lengths of the alternative paths are invariably greater than the path including wormhole tunnel. The basic idea behind this approach is illustrated in below section.

The objective of this research was to detect and prevent wormhole attacks in AODV routing protocol which has been done in the proposed technique based on hop count analysis approach. The basic idea behind the proposed technique is using hop count as a parameter to distinguish paths containing wormhole tunnel.

The basic idea of hop count analysis is illustrated in figure 3.1. Mostly the routes contain larger hop count value for example hop count value is 5 and 6 in the network shown in figure, to establish connection between source node and destination node. While the hop count value of the path going through wormhole tunnel will be much smaller, in this case the value of hop count is 2. It can be explained as, consider a source node which wants to communicate with a destination node. If source node communicates through the wormhole tunnel then it encounters only 2 hops. But the other possible alternative routes comprise 5 or 6 hops to transfer a packet from the same source to destination nodes. Thus it can be a basic approach that the route path having too small hop count value or the path having invariably smaller number of hops may be unsafe. So the proposed technique is that by avoiding the route paths having too short hop count value the wormhole tunnel can be kept away.

In the proposed detection technique, hop count values of all the available route paths is calculated first. Source node then verifies the one hop neighbours and accordingly a threshold value is set, which is used for comparing the number of hops of the current route with the next available route. If the length of the new route differs extensively compared to the length of the preferred path followed by AODV then it can be concluded as a wormhole attack.

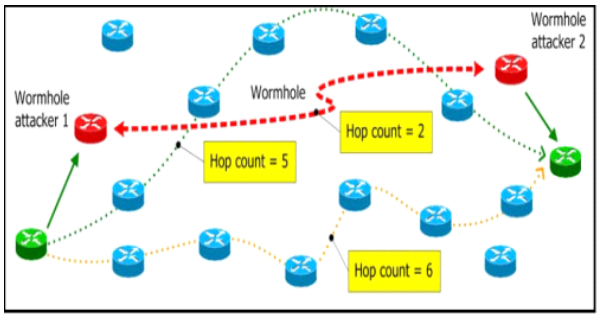


Figure 4.1 Compare hop count values of all available routes linking source node and destination node

Algorithm of the proposed hop count based detection technique

In the proposed technique, any node not necessarily the source node, which is set in detect mode uses this hop count analysis approach to detect and prevent wormhole attack. Whenever any node sends the RREQ packets and in turn start receiving RREP packets, it follows the below mentioned algorithm using the checkpath( ) function module in AODV routing protocol implemented in ns-2.

The algorithm is repeatedly executed in ns-2 in every 0.1 seconds. The purpose of repeatedly checking the routes is to ensure that the wormhole attacker nodes should not get included in the selected path for packet transmission from source to destination because of the RREP packet sent by the malicious nodes. This is possible because the malicious node sets the highest sequence number and lowest hop count which is one in the RREP packet.

Hop-count Analysis Algorithm:

- To detect wormhole in AODV, all the available paths to the destination are checked one by one through routing table.
- To check the paths, AODV determines number of hops and each one-hop neighbor is verified.
- If there is one hop neighbour, it is legitimate and threshold is incremented by 1, otherwise it is decremented. This way a threshold value is set.
- Then the next alternative path is checked in similar manner and number of hops is calculated which again defines a new threshold value.
- Source node compares length of selected route with alternative path by comparing number of hops and threshold.
- If the number of hops of the considered route is greater than the set threshold, it is concluded that wormhole exists.
- On detecting malicious route, the corresponding next hop entry is deleted, so that now that suspected neighbour is not used for routing.
- Similarly other paths are examined using the step 5 – 10.

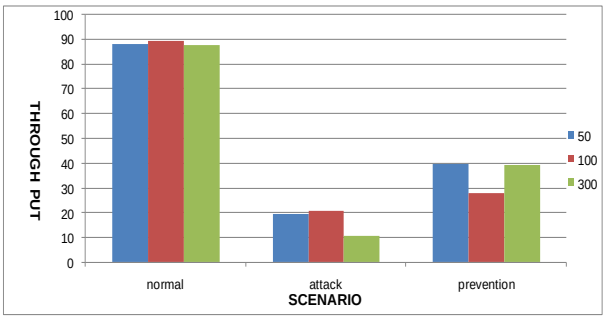
DOI 10.17148/IJARCCE.2015.41276

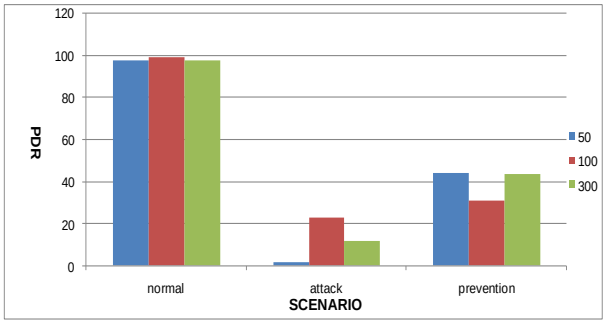
IJARCCE

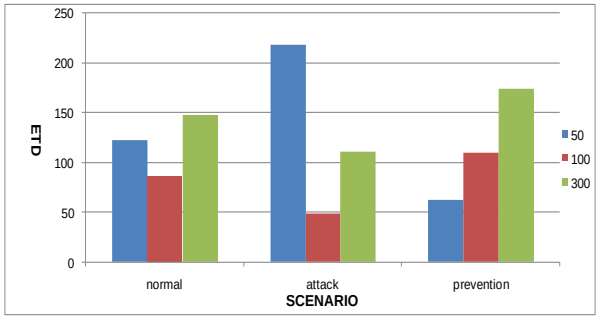
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Results







7. CONCLUSION

The research work proposes a solution based on specification-based intrusion detection technique to monitor the AODV routing protocol and detect wormhole attack on AODV. The proposed approach involves the use of a counter for specifying correct AODV routing behavior and individual nodes monitor the routing behavior of their neighbors for detecting run-time violation of the specifications. In addition, one additional field, count in the RREP message is proposed to enable the monitoring. Another important modification is that RREP packets are broadcasted as opposed to unicast to the source in normal AODV.

REFRENCES

1. M .Sookhak ,M.R. Eslaminejad, M. Haghparastand I.in FauziISnin ―DetectionWormhole in Wireless Adhoc networks ‖IJCST , Volume 2, Issue 7, October (2011).
2. Mr. SusheelKumar , Vishal Pahal , SachinGarg ―Wormholeattack in Mobile AdHoc Network ", IRACST – Engineering Scienceand Technology: An International Journal (ESTIJ), ISSN:2250 3498,Vol.2, No. 2, April (2012)
3. Marianne Azer, Sherif El-Kassas and Magdy El-Soudani ―A Full Image of the Wormhole Attacks towards Introducing Complex Wormhole Attacksin wireless Ad Hoc Networks‖ in (IJCSIS) International Journal of Computer Science and Information Security, Vol. 1, No. 1, May (2009).
4. Ramandeep Kaur, Jaswinder Singh ―Towards Security against Malicious Node attack in mobile adhocnetwork‖ , in IJARCSSE, ISSN: 2277 128X , Volume 3, Issue 7,July2013.
5. MajidMeghdadi, SuatOzdemir and InanGüler ―A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks‖ ,in IETETECHNICAL REVIEW,VOL 28 , ISSUE 2 ,MAR-APR 2011.
6. JyotiThalor ,Ms. Monika ―Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks‖, in Volume 3,Issue 2, February 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering(2013).
7. R.Sherine Jenny, N.Sugirtham― simulation based performance comparision of F AODV, DSR, FSR routing protocol with worm hole attack "in IRACST – International Journal of Computer Networks and Wireless Communications(IJCNWC), ISSN: 2250-3501 Vol.3, No1, February (2013).
8. Vandana C.P, Dr. A. Francis Saviour Devaraj ―Evaluation of Impact of Wormhole Attack on AODV" in Int. J. Advanced Networking and Applications Volume: 04 Issue:04 1652-1656 ISSN : 0975-0290(2013).
9. SudhirAgrawal, Sanjeev Jain, and Sanjeev Sharma "Asurvey of routing attacks and Security measures in mobile Adhoc networks" in journal of computing volume 3, issue, ISSN 2151- 9617 1,January (2011).
10. MangeshGhongeandProf. S. U.Nimbhorkar "Simulation of AODV under Blackhole Attack in MANET" in InternationalJournal of Advanced Research in Computer Science and Software EngineeringVolume 2, Issue 2,ISSN: 2277 128X February (2012).
11. MohitJain and HimanshuKandwal ―A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks in 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies978-0-7695-3915-7/09 $26.00 (2009).
12. KhinSandar Win ―Analysis of Detecting Wormhole Attackin Wireless Networks‖ in World Academy of Science, Engineering and Technology 24(2008).
13. YudhvirSingh,AvniKhatkar, Prabha Rani, Deepika, and DheerDhwaj Barak ―Wormhole Attack Avoidance Technique in Mobile Adhoc Networks‖ in IEEE 978-0-7695-4941-5/12 $26.00 (2013).
14. Ian F. Akyildiz ,Xudong Wang , and Weilin Wang ―Wireless mesh networks: a survey‖ in Elsevier Computer Networks 47 -445–487(2005).
15. Youngho Cho and Gang Qu and Yuanming Wu ―Inside Threats against TrustMechanism with Watchdog and Defending Approaches in Wireless Sensor Networks‖ IEEE CSSecurity and Privacy Workshops (2012).
16. PriyaMaidamwar and NekitaChavhan ― A survey on security issues to detect wormholeattacks in wireless sensor network‖ in International Journal on Ad Hoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012.
17. Pushpendra Niranjan, Prashant Srivastava, Raj kumar Sonand Ram Pratap ―Detection of wormhole attack using hop count andtime delay analysis‖ in International Journal of Scientificand Research Publications, ISSN 2250-3153,Volume 2, Issue 4, April 2012.
18. Ajay PrakashRai, Vineet Srivastava and Rinkoo Bhatia ―Wormhole Attack Detection in Mobile AdHoc Networks" in International Journal of Engineering and Innovative Technology (IJEIT), ISSN: 2277-3754, Volume 2, Issue 2, August 2012.