IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 5, Ver. V (Sep. - Oct. 2016), PP 32-38
www.iosrjournals.org

Prevention and Detection of Wormhole Attack in Mobile Adhoc Network Using Clustering and RTT

Reena Shakya[1], Nitesh Gupta[2]
[1]*M.Tech Research Scholar Department of Computer Science and Engineering, Institute of Information Science & Technology, Bhopal*
[2]*M.Tech Research Guide Department of Computer Science and Engineering, Institute of Information Science & Technology, Bhopal*

Abstract: *A security constraint in mobile adhoc network is very critical task. Some critical security issue such as black hole attack, wormhole attack, sinkhole attack, prevention and detection of attack is major challenge. For the detection of wormhole attack various authors used various technique such as clock synchronization, threshold based technique, nearest neighbor node selection method. In this dissertation modified the IMAODV protocol in terms of IMAODV protocol.In this paper modified the AODV routing protocol for the detection of wormhole attack. The modified protocol is called secured energy efficient routing protocol (IMAODV). The IMAODV protocol based on two functions one is threshold based function and one is energy based function. The threshold based function measure the distance of normal node and wormhole node. Our proposed algorithm is very efficient in compression in ADOV routing protocol.*

Keywords: *MANET, AODV, IMAODV.*

I. Introduction

In this paper proposed a secured AODV routing protocol for the prevention and detection of wormhole attack. The dynamic infrastructure of mobile ADHOC network creates some security issue in network. A security constraint in mobile adhoc network is very critical task. Some critical security issue such as worm hole attack, wormhole attack, sinkhole attack, prevention and detection of attack is major challenge. For the detection of wormhole attack various authors used various technique such as clock synchronization, threshold based technique, nearest neighbor node selection method. In this dissertation modified the IMAODV protocol in terms of SEAODV protocol. Also increase the life of network for the purpose of communication. If in network attack is performed the consumption of power is increase. The process of detection cum prevention used clustering technique and round trip time. The round trip time basically based on the concept of single hop technique, the measurement of single hop node concept measured with the process of time to live of communication node. For the process of clustering used partition clustering technique for the grouping of round trip time for the cluster generation.Interest in such networks has recently grown due to the common availability of wireless communication devices that can connect laptops and palmtops and operate in license free radio frequency bands (such as the Industrial-Scientific- Military or ISM band in the U.S.). In an interest to run internetworking protocols on ad hoc networks, a new working group for Mobile, Ad hoc Networking (MANET) has been formed within the Internet Engineering Task Force (IETF), whose charter includes developing a framework for running IP based protocols in ad-hoc networks. Interest has also been partly fueled by the recent IEEE standard 802.11 that include the MAC and physical layer specifications for wireless LANs without any fixed infrastructure. Routing protocols in packet-switched networks traditionally use either link-state or distance-vector routing algorithm. Both algorithms allow a host to find the next hop neighbor to reach the destination via the "shortest path." The shortest path is usually in terms of the number of hops; however, other suitable cost measures such as link utilization or queuing delay can also be used. Such shortest path protocols have been successfully used in many dynamic packet switched networks. Prominent examples include use of link state protocol in OSPF (Open Shortest Path First) [9] and use of distance vector protocol in RIP (Routing Information Protocol) for interior routing in the Internet. Even though, any such protocol would, in principle, work for ad hoc networks, a number of protocols has been specifically developed for use with ad hoc networks. The rest of paper organized in section II some attack in section III routing protocol in section IV discuss the proposed method in section V simulation result and finally discuss conclusion and future scope.

II. Security Issues In Mobile Ad Hoc Network

MANET is vulnerable to various types of attacks. Some attacks affect to general network, some affect to wireless network, and some are particular to MANETs [5, 7]. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks. These security attacks in MANET and all other networks can be generally classified by the following criteria: passive

or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related.

- **Passive vs. active attacks:**

The attacks in MANET can generally be classified into two major categories, namely passive attacks and active attacks [6, 7]. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring. Examples of active attacks include jamming, impersonating, modification, denial of service (DoS), and message replay.

- **Internal vs. external attacks:**

The attacks can also be classified into external attacks and internal attacks, according the domain of the attacks. Nodes that do not belong to the domain of the network carry out external attacks [6, 7]. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more harmful when compared with outside attacks since the insider knows valuable and secret information, and possesses confidential access rights.

- **Eavesdropping:**

Eavesdropping is the intercepting and reading of messages and conversations by unintended receivers [5, 6]. The mobile hosts in mobile ad hoc networks share a wireless medium. The majorities of wireless communications use the RF spectrum and broadcast by nature. Signals broadcast over airwaves can be easily intercepted with receivers tuned to the proper frequency. Thus, messages transmitted can be overheard, and fake messages can be injected into network.

- **Interference and Jamming:**

Radio signals can be blocked or interfered with, which causes the message to be corrupted or lost [5, 7]. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. The most common types of this form of signal jamming are random noise and pulse.

- **Black hole attack:**

The black hole attack has two properties [6, 8]. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is false, with the intention of intercepting packets. Second, the attacker consumes the intercepted packets without any forwarding.

- **Byzantine attack:**

A compromised intermediate node works alone[6, 7], or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

- **Rushing attack:**

Two colluded attackers use the tunnel procedure to make a wormhole. If a fast transmission path exists between the two ends of the wormhole, the tunneled packets can transmit faster than those through a normal multi-hop route [6]. This forms the rushing attack. The rushing attack can act as an effective denial-of- service attack against all currently proposed on-demand MANET routing protocols.

III. Routing Protocols

In order to facilitate communication within the network, a routing protocol is used to discover routes between nodes. The primary goal of such an ad-hoc network routing protocol is correct and efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. Route construction should be done with a minimum of overhead and bandwidth consumption.

An Ad-hoc routing protocol is a convention or standard that controls how nodes come to agree which way to route packets between computing devices in a MANET. In ad-hoc networks, nodes do not have a priori knowledge of topology of network around them, they have to discover it.

The basic idea is that a new node announces its presence and listens to broadcast announcements from its neighbors. The node learns about new near nodes and ways to reach them, and announces that it can also

reach those nodes. As time goes on, each node knows about all other nodes and one or more ways how to reach them.

Routing algorithms have to:

- Keep routing table reasonably small
- Choose best route for given destination (this can be the fastest, most Reliable, highest throughput, or cheapest route)
- Keep table up-to-date when nodes die, move or join
- Require small amount of messages/time to converge

In a wider context, an ad-hoc protocol can also mean an improvised and often impromptu protocol established for a particular specific purpose. Since the advent of DARPA packet radio networks in the early 1970s, numerous protocols have been developed for ad-hoc mobile networks. Such protocols must deal with the typical limitations of these networks, which include high power consumption, low bandwidth, and high error rates. As shown in Figure 1 below, these routing protocols may generally be categorized as: (a) table-driven and (b) source-initiated on-demand driven. Solid lines in this figure represent direct descendants while dotted lines depict logical descendants. Despite being designed for the same type of underlying network, the characteristics of each of these protocols are quite distinct.

IV. Proposed Method

The proposed algorithm is combination of cluster based algorithm and single hop concept. The single hop communication differentiates the process of request and response for the process of wormhole attack. The process of wormhole attack identifies by the process of multiple round trip time. If the request is multiple in single node as hop generate the phase of cluster and identify as attack.

Algorithm process for cluster
Begin
Step1: call RTP ()
Step 2: for k: =1 to n-1
Call update cluster according to RTP
Send message to all mobile node
Endfor
Step 3 create control message
Step 4 communicate all node
Here initialed three condition for the detection of wormhole node

i. Node have multiple hops
ii. Node have maximum RTT
iii. Node have stable.

1st condition process
Begin
Create count of hop
Set n= current node
Set F=ture
Add node id
Return end
2nd condition
If (n=true)
Then if (fail N !N)
Then create new hop
Endif
Else
Add another hop
Endif
End
3rd condition
Wormhole= node id
Change the hop count
Connect the node
Return
End.

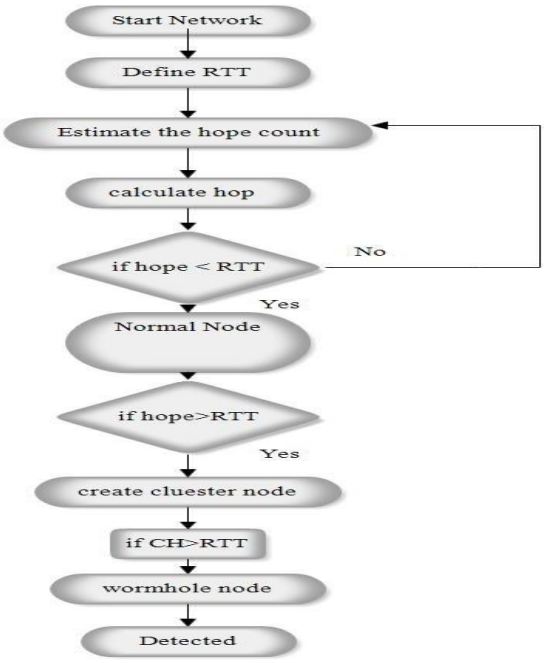

Figure 1: proposed model of wormhole detection based on RTT.

V. Result Analysis

To investigate the effectiveness of the proposed scheme for improvement of performance of MANET network using IMAODV routing protocol on a simplified topology was carried out using Network Simulator version 2.34.

Table 1 simulation parameter

Parameter	value
Simulation duration	50,100.150, 200 sec
Simulation area	1000*1000
Number of mobile node	10,20,30,40,50
Traffic type	Cbr(udp),
Packet rate	4 packet/sec
Abnormal node	Variable
Host pause time	10sec

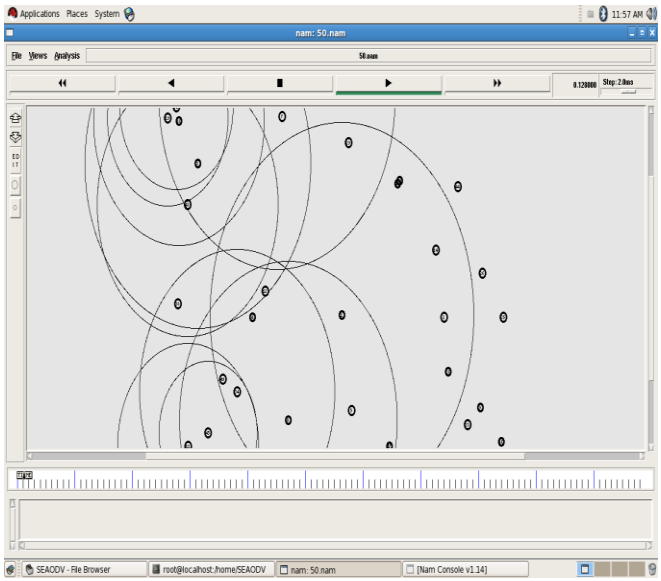

Figure 2: simulation scenario of AODV-MANET scheme on pause time 40 s. in this scenario used 25 normal nodes and 2 worm node for the process of attack scenario. The 2 worm node decades the path length for the neighbor's node.

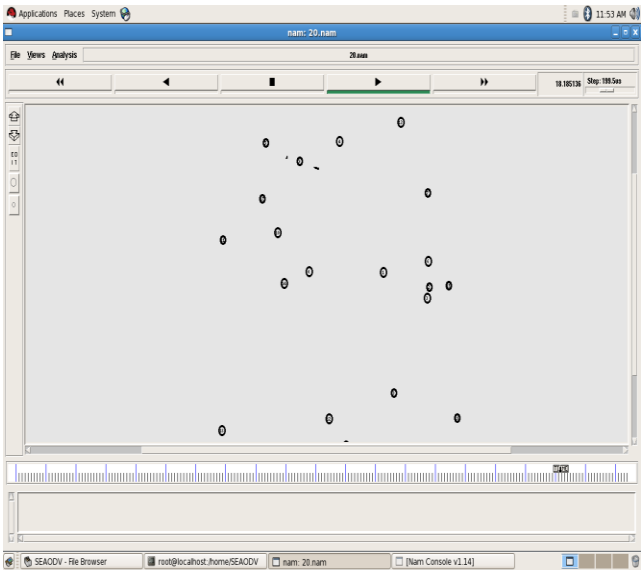

Figure 3: simulation scenario of AODV-MANET scheme shows the packet. In this scenario of network shows that the IMAODV protocol for the prevention of worm hole node. This scenario prevents the worm hole attack and there is no any packet dropping occurred during the process of communication.

Table 2: Shows that the comparative result of PDR value using AODV and IMAODV methods

NO. Of NODE	Value of PDR	
	AODV	IMAODV
10	0.55	0.65
20	0.52	0.62
30	0.40	0.43
40	0.30	0.35
50	0.34	0.35

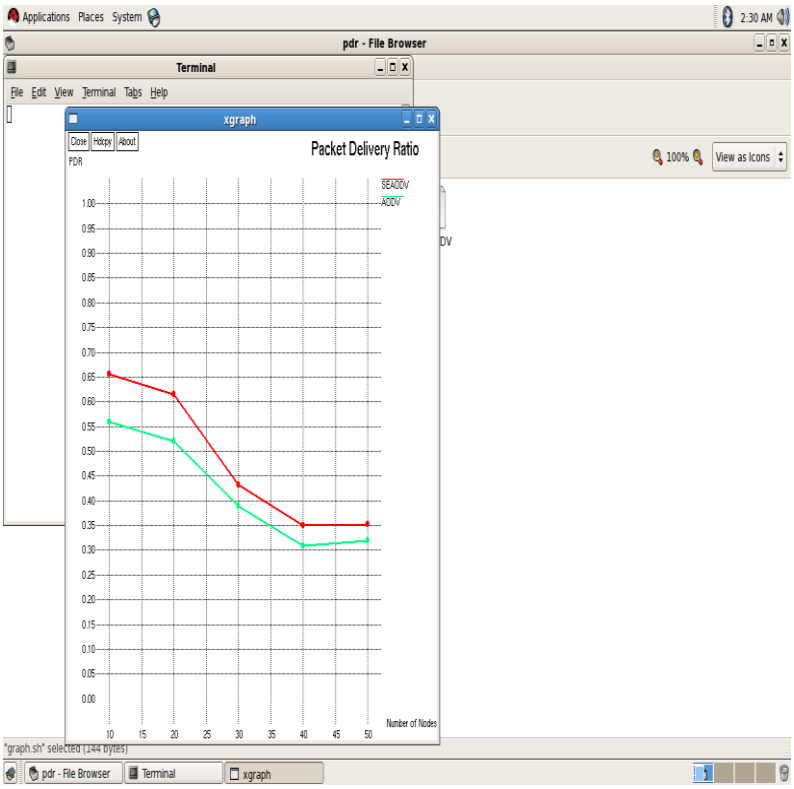

Figure 4: describe the simulation result of packet delivery ratio between IMAODV and AODV protocol. the graph plot between number of node and delivery ratio of packet. The graph shows that the IMAODV protocol is much better than AODV protocol.

Table 3: Shows that the comparative result of Average End to End Delay value using AODV and IMAODV methods

NO. Of NODE	Value of Avg End to End Delay	
	AODV	IMAODV
10	0.025	0.020
20	0.360	0.260
30	0.580	0.480
40	0.510	0.410
50	0.400	0.390

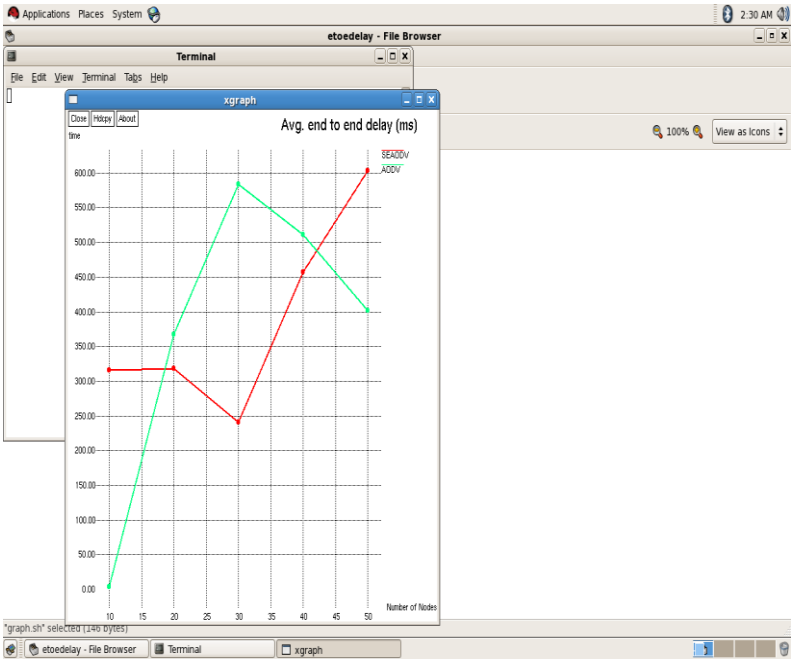

Figure 5: describe the performance of end to end delivery ratio of packet in both protocol AODV and IMAODV. The prevention process of IMAODV is call the delay of packet is reduces and increase the efficiency of hop count. The number of hop count is reducing then the delay of network is decrease.

VI. Conclusion & Future Scope

In this papermodified the AODV routing protocol for the detection of wormhole attack. The modified protocol is called improved efficient routing protocol (IMAODV). The IMAODV protocol basically based on two function one is RTT function and other is clustering process. The function of RTT estimate the hop of routing load during the process of communication. The estimated value of RTT proceed for the generation of cluster. The cluster estimated the value of normal node and abnormal node. The modified and improved AODV protocol is better than AODV protocol. The RTT and clustering technique is good technique for wormhole detection technique. in future this algorithm is used for real time scenario of wormhole detection.

References

[1]. Amrit Suman, Praneet Saurabh and BhupendraVerma. A Behavioral Study of Wormhole Attack in Routing for MANET. International Journal of Computer Applications, 2011.
[2]. YANZHI REN, MOOI CHOO CHUAH, JIE YANG and YINGYING CHEN. DETECTING WORMHOLE ATTACKS IN DELAY-TOLERANT NETWORKS, IEEE, 2010.
[3]. Sweety Goyal and Harish Rohil. Securing MANET against Wormhole Attack using Neighbor Node Analysis. International Journal of Computer Applications. 2013.
[4]. Anil Kumar Fatehpuria and Sandeep Raghuwanshi. An Efficient Wormhole Prevention in MANET Through Digital Signature. International Journal of Emerging Technology and Advanced Engineering. 2013.
[5]. Priyanka Goyal, VintiParmar and Rahul Rishi, MANET: Vulnerabilities, Challenges, Attacks, Application, IJCEM, 2011.
[6]. Issa Khalil, Saurabh Bagchi, Cristina N. Rotaru and Ness B. Shroff, UNMASK: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks, Elsevier, 2010.
[7]. Mina Rahbari and Mohammad Ali JabreilJamali, EFFICIENT DETECTION OF SYBIL ATTACK BASED ON CRYPTOGRAPHY IN VANET, IJNSA, 2011.
[8]. Debdutta Barman Roy, RituparnaChaki and NabenduChaki, A NEW CLUSTER-BASED WORMHOLE INTRUSION DETECTION ALGORITHM FOR MOBILE AD-HOC NETWORKS, International Journal of Network Security & Its Applications, 2009.
[9]. Saurabh Gupta, SubratKar and S Dharmaraja, WHOP: Wormhole Attack Detection Protocol using Hound Packet", International Conference on Innovations in Information Technology, 2011.

[10]. PushpendraNiranjan, Prashant Srivastava, Raj kumarSoni and Ram Pratap, Detection of Wormhole Attack using Hop-count and Time delay Analysis, International Journal of Scientific and Research Publications, 2012.
[11]. Sanjay Kumar Dhurandher, Isaac Woungang, Abhishek Gupta and Bharat K. Bhargava, E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks, IEEE, 2012.
[12]. Saurabh Upadhyay and ArunaBajpai, Avoiding Wormhole Attack in MANET using Statistical Analysis Approach, International Journal on Cryptography and Information Security, 2012.
[13]. Jaspal Kumar, M. Kulkarni and Daya Gupta, Effect of Black Hole Attack on MANET Routing Protocols, MECS, 2013.
[14]. Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, MANET Routing Protocols and Wormhole Attack against AODV, IJCSNS, 2010.
[15]. Ajay Prakash Rai, Vineet Srivastava and Rinkoo Bhatia "Wormhole Attack Detection in Mobile Ad Hoc Networks", IJEIT, 2012, Pp 174-179.
[16]. Samir Das, Charles E. Perkins, Elizabeth M. Royer, and Mahesh K. Markina. Performance comparison of two on-demand routing protocols for ad hoc networks. IEEE, 2008.
[17]. Benjie Chen, Kyle Jamieson, Hari Balakrishnan, and Robert Morris. Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks. In Mobile Computing and Networking, 2012.
[18]. Qun Li, Javed A. Aslam, and Daniela Rus. Online power-aware routing in wireless ad-hoc networks. In Mobile Computing and Networking, 2001.
[19]. Ya Xu, John S. Heidemann, and Deborah Estrin. Geography-informed energy conservation for ad hoc routing. In Mobile Computing and Networking, 2007.
[20]. Suresh Singh, Mike Woo, and C. S. Raghavendra. Power-aware routing in mobile ad hoc networks. In Mobile Computing and Networking, 2005.
[21]. JyhSivalingam, K. Agrawal, and M. Srivastava. Design and analysis of low-powerAccess protocols for wireless and mobile atm networks. Wireless Networks, 2000.
[22]. Tamer A. ElBatt, Srikanth V. Krishnamurthy, Dennis Connors, and Son K. Dao. Power management for throughput enhancement in wireless ad-hoc networks. In ICC (3), 2000.
[23]. Laura Marie Feeney and Martin Nilsson. Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. In IEEE INFOCOM, 2001.
[24]. Zhengming Li and ChunxiaoChigan" AWF-NA: A Complete Solution for Tampered Packet Detection in VANETs" in IEEE conference 2009.
[25]. SoufieneDjahel, FaridNa¨ıt-abdesselam, and Zonghua Zhang "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" in IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011.