VOL. 11, NO. 21, NOVEMBER 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ASCERTAINMENT OF WORMHOLE AND BLACK HOLE ATTACKS IN MANET USING DOWB ALGORITHM

Pavan Kumar T, Srikanth. V and Latha Reddy B
Department of Computer Science Engineering, K L University, Guntur, India
E-Mail: pavankumar_ist@kluniversity.in

ABSTRACT

The omnipresent nature of mobile devices gaggle canvassers (researchers) into investigating how these expedients can be exploited and assimilated into education methods. Particularly, ad-hoc networks have been gaining attractiveness for applications requiring rapid deployment. Investigators have exasperated to propose protocols that will develop the quality of service for ad-hoc networks in the inimical wireless milieus. A lot of applications, predominantly army applications, oblige great security considerations. Consequently, the significant challenging issue is to guard ad-hoc networks from security assaults. The key property in ad-hoc networks is usage of exposed wireless medium for communion. Resulting that intruder feels easy to inauguration attacks by injecting, altering, tampering the data items. Each device in the network works as router as well host it makes confusion to insert a firewall device. Considering about different network layer attacks in MANETS principally two attacks cause big damage to communication over ad- hoc network. Those are wormhole or collider attack and black hole attack. In this article we propose a new algorithm to detect black hole and wormhole attacks in MANET. And we evaluate the performance using NS-2.

Keywords: NS-2, MANET, black hole, ad-hoc networks.

1. INTRODUCTION

The spread in portable and wireless communication technologies fashioned newfangled milieus that combine actual biosphere and alphanumeric world learning resources. The omnipresent nature of mobile devices gaggle canvassers (researchers) into investigating how these expedients can be exploited and assimilated into education methods. Particularly, ad hoc networks have been gaining attractiveness for applications requiring rapid deployment. Investigators have exasperated to propose protocols that will develop the quality of service for ad hoc networks in the inimical wireless milieus. A lot of applications, predominantly army applications, oblige great security considerations. Consequently, the significant challenging issue is to guard ad hoc networks from security assaults.

The key property in ad-hoc networks is usage of exposed wireless medium for communion. Resulting that intruder feels easy to inauguration attacks by injecting, altering, tampering the data items. Each device in the network works as router as well host it makes confusion to insert a firewall device. Considering about different network layer attacks in MANETS principally two attacks cause big damage to communication over ad hoc network. Those are wormhole or collider attack and black hole attack; collider attack is composed with two or more collider nodes and a high speed connection over other connected hosts. Black hole is a single host and it having a property that drops all the data items against the protocol. In this article we propose a mechanism to detect the both wormhole and black hole attack. And we illustrate the performance of routing protocol before and after detection mechanism. And the implementation is taking place using NS2. This article is organized as follows section-1 gives brief introduction, section-2 gives the different existing methods, section-3 deals with proposed method, section -4 describes the experimental evaluation and finally section-5 concludes the paper.

2. RELATED WORK

In wormhole recognition technique taking into account round outing time (RTT) and neighbor number is exhibited. At the point when the RTT between two hubs is impressively more noteworthy, they check the neighbor number. In the event that the estimation of neighbor number is more prominent than the normal neighbor number, there is a suspect that a wormhole connection is in the middle. This strategy expects that all system hubs utilize the same equipment and programming arrangement. In addition, they compute the normal number of came to before the timeout interim, the originator positions the hub as suspicious and stops neighbors utilizing an equation, which is more relevant when the system hubs are uniformly disseminated [1]. The creators proposed a wormhole location technique, which endeavors to pinpoint wormhole joins before applying the recognition systems. In the event that HELLO rep from a hub is not correspondence with it until the end of wormhole confirmation process. In the confirmation stage the originator sends examining parcels to every one of the suspicious hubs [6]. In any case, both periods of this wormhole identification strategy rely on upon postponement just components, which might create more prominent false caution rate.

2.1. AODV routing protocol

AODV is a dynamic routing protocol it will arranges routs on ultimatum from source to the target. AODV mainly deliberate for to switch the problems of titanic message header in on plea protocols and enormous packet overhead due to the sporadic apprise messages in fixed routing protocols. Operational of AODV is essentially tranquil with two level's one is direction

discovery and one more is direction maintenance. Predominantly, it habits comprehensive direction discovery method by broadcasting R_REQ message over the network for to verdict preferred route to the target. Whenever the target gets the R_REQ from the neighbor it reiterates back to the initiator with R_REP.

After getting R_REP message form the target the route is well-established, and transmission of data takes place. Secondarily, route maintenance is composed with three operations route error, hello and time out messages. Route error message is fired when the route is not available or failed. Hello is used to check the connection condition and time out is used to identify the connection status, if a connection is inactive, it will be discorded after timeout completion [2].

2.2. AODV with black hole and wormhole attacks:

AODV routing is completely disturbed when there is a black or wormhole in the network. Both black hole and Worm hole attacks are propelled during the direction discovery practice, a knob wants to communicate with other node normally this conversation is possible with shortest path which is provided by the AODV, that route is called as traditional route. If mugger is present in the network the route is always initiated through the noxious nodes to make communication with the destination, this path is called as attacker's path [6]. It illuminates that attack is wholly aggravate AODV routing. Due to network layer attacks QOS performance parameters are exaggerated tremendously, those are throughput, jitter, packet delivery ratio and end to end delay [3].

Node id	
HOP Count	List of first hop neighbors
No of packets received from its first hop neighbors	No of packets transfers

3. PROPOSED ALGORITHM: (DOWB)

Algorithm to detect wormhole and black hole attacks in AODV routing protocol
The algorithm proceed as follows

Step 1:

Identifying reliable, moderate reliable and not reliable

Step 2: Locating of attacker nodes based on statistical analysis for to identify the reliability of a node in the network we use status table at the node. And also we are considering the energy level of a node. From the status Table first we finds the ratio for number of transferred packets to the number of received packets.

T_h $=NT_p/NR_P$
T_h = Threshold value
NT_p = Number of packets transferred
NR_p = Number of received packets

If T_h value is between0.8 to 1 and energy level is green/yellow/red zone then the node is reliable.

If T_h value is between0.6 to 0.8 and energy level is yellow/red zone then the node is moderate reliable.

If T_h value is between0.1 to 0.4 and energy level is red zone then the node is not reliable.

Step 3:

Identify the nodes which are moderate reliable and not reliable test the paths twice by broadcasting of RREQ message and identify the hop count and RTT.

If path length less (that if the path is established with the less number of nodes may existence of worm hole nodes) and also calculate the RTT. Compare the RTT of reliable nodes path and others (i.e. moderate reliable and not reliable nodes). RTT varies drastically then the nodes are treated as attackers.

By avoiding of those nodes AODV works efficiently.

4. EXECUTION EXAMINATION

The reproductions were performed utilizing Network Simulator 2 of version 2.35. Arbitrary waypoint model is utilized to produce the versatility situations by fluctuating number of hubs (10, 30 and 50) moving in a region of 1000 X 800 meters. Hear we utilizes sufficient bundle rate and whimsical delay times to reproduction and we implement DOWB technique to detect both the black hole and wormhole nodes in the network and compare the performance of the AODV routing protocol with B-W AODV and DOWB AODV by capricious the number of attacker nodules in the set-up. And we appraise innumerable enactment metrics of packet conveyance portion, throughput and end to end delay. The reproduction parameters are abridged in Table 1.

4.1. Performance metrics

4.1.1. Packet delivery fraction: It is the proportion of aggregate number of bundles got to the aggregate number of parcels exchanged.

4.1.2. Throughput: Quantity of sachets transferred in unit time from home to target is called throughput.

4.1.3. End to end delay: The time taken by a packet transferred from source to destination is called end to end delay

Parameter	Values
Traffic type	CBR.
Number of nodes	10, 30 and 50.
Simulation time	2000 sec.
Pause time	0, 1, 2, 3, 4 and 5.
Simulation area	1000 X 800 meters.
Mobility	0 to 25 meter/sec.
Performance metrics	PDF, Throughput and E2E Delay

5. RESULT ANALYSIS

In this article we assess performance of traditional AODV, AODV with the network layer attacks of black hole and colliding attacks and after detection of these attacks under three measures those are throughput, E2E Delay and PDF.

Figure-2, Figure-3, and Figure-4 shows the throughput comparison of normal AODV, AODV under attacks and after attack detection. DOWB algorithm detects all most all attacker nodes that prove the throughput after the detection of attackers near to the normal AODV.

Figure-5, Figure-6, and Figure-7 shows the E2E delay comparison of normal AODV, AODV under attacks and after attack detection. DOWB algorithm detects all most all attacker nodes that prove the end to end delay after the detection of attackers near to the normal AODV.

Figure-8, Figure-9, and Figure-10 shows the packet delivery ratio comparison of traditional AODV, AODV under attacks and after attack detection. DOWB algorithm detects all most all attacker nodes that prove the packet delivery fraction after the detection of attackers near to the normal AODV.

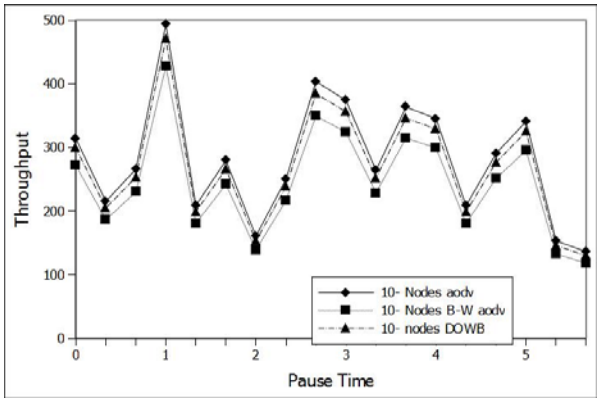

Figure-1. 10-Nodes Throughput.

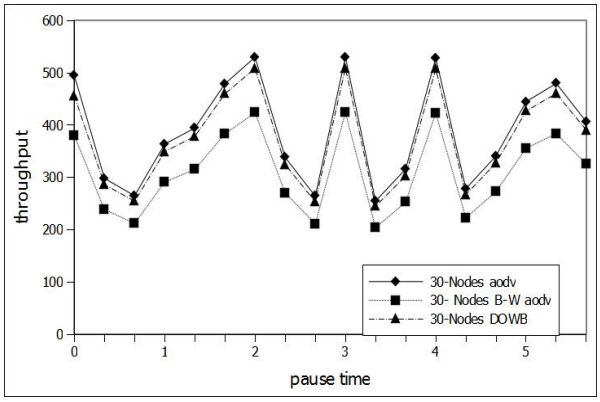

Figure-2. 30-Nodes throughput.

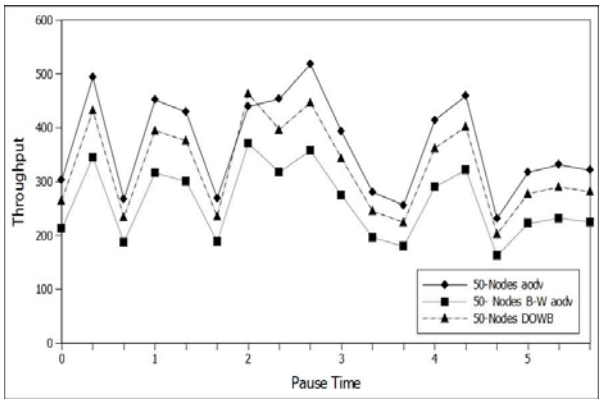

Figure-3. 50-Nodes throughput.

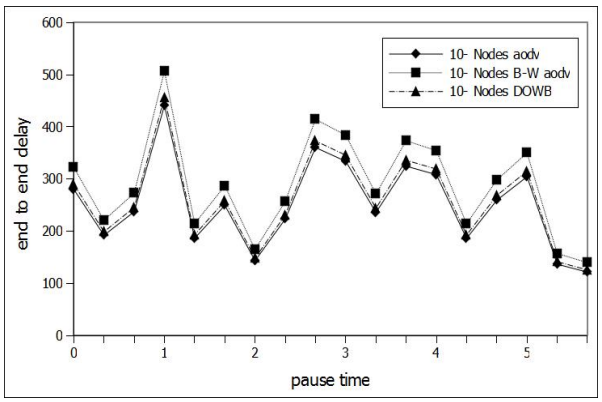

Figure-4. 10-Nodes End To End Delay.

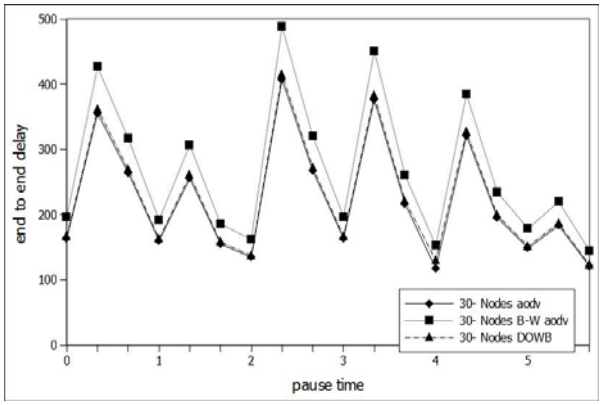

Figure-5. 30-Nodes End to End Delay.

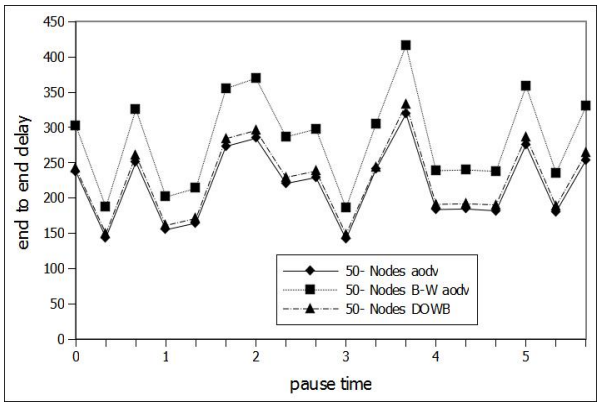

Figure-6. 50-Nodes end to end delay.

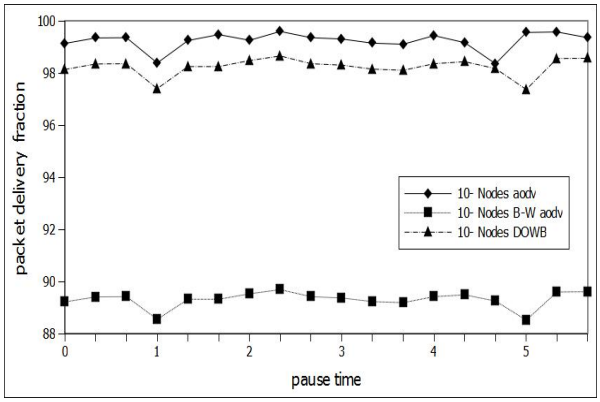

Figure-7. 10-Nodes packet delivery ratio.

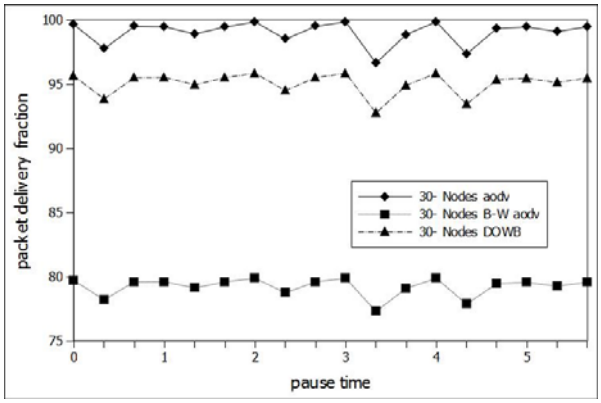

Figure-8. 30-Nodes packet delivery ratio.

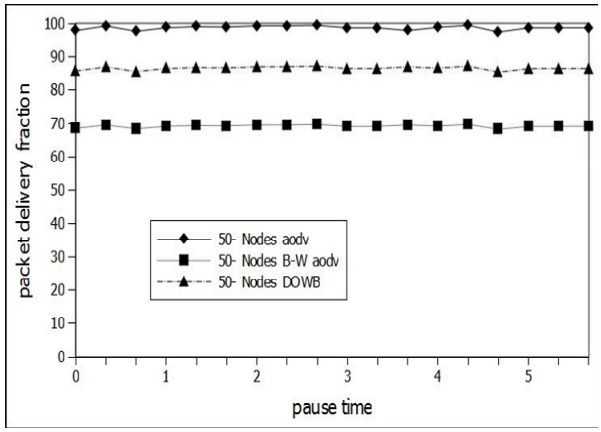

Figure-9. 50-nodes Packet delivery ratio.

6. CONCLUSIONS

This paper proposed a technique named DOWB which detects the network layer attacks of black hole and wormhole attacks in MANET. To appraise the enactment of proposed methods, simulation of all drop and collider attacks along with the simulation of proposed techniques had been done. The enactment results show that DOWB successfully detect and avoid the attackers from routing.

REFERENCES

[1] C.E. Perkins. 2000. Ad Hoc Networking. Addison-Wesley Professional, first edition.

[2] S. Basagni, M.Conti, S. Giordano and I. Stojmenovic. 2004. Mobile Ad Hoc Networking. A. John Wiley and Sons, Inc., Publication, ISBN 0- 471-37313-3.

[3] E.S. Babu. 2013. An Implementation and Performance Evaluation Study of AODV, MAODV, RAODV in Mobile Ad hoc Networks. 4(9): 691-695.

[4] Thaier Hayajneh, Prashant Krishnamurthy, David Tipper. 2009. DeWorm: A Simple Protocol to Detect Wormhole Attacks in Wireless Ad hoc Networks. 978-0-7695-3838-9/09 $26.00 © 2009 IEEE

[5] E.S. Babu and M.L.R. Chandra. 2012. A comprehensive study of Routing protocols in Mobile Ad hoc Networks: Research Survey. 7(7): 77-83.

[6] A. Peda Gopi, E. Suresh Babu, C. Naga Raju, S. Ashok Kumar. 2015. Designing an Adversarial Model against Reactive and Proactive Routing Protocols in MANETS: A Comparative Performance Study. International Journal of Electrical and Computer Engineering (IJECE). 5(5): 1111~1118 ISSN: 2088-8708

[7] S. Ashok Kumar, E. Suresh Babu, C. Nagaraju, A. Peda Gopi. 2015. An Empirical Critique of On-Demand Routing Protocols against Rushing Attack in MANET. International Journal of Electrical and Computer Engineering (IJECE). 5(5): 1102~1110 ISSN: 2088-8708.

[8] Sunil Taneja, and Ashwani Kush. 2010. A Survey of Routing Protocols in Mobile Ad Hoc Networks. International Journal of Innovation, Management and Technology. 1(3), ISSN: 2010-0248.

[9] E.S. Babu, C. Nagaraju, and M.H.M.K. Prasad. 2013. A Comparative Study of Tree based Vs. Mesh based Multicast Routing Protocols in Mobile Ad hoc Networks. 2(6): 6-11.

[10] T.P. Kumar, E. Suresh, B.V. Ramana, and B.S. Shashank. 2015. Survey: Routing Protocols in Cognitive Radio Mesh Networks. 6(1): 603-608

[11] Farid Na¨ıt-Abdesselam, Brahim Bensaou and Jinkyu Yoo1. 2007. Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol. IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings.

[12] D.B. Johnson, D.A. Maltz, Y. Hu and J.G. Jetcheva. 2002. The dynamic source routing protocol for mobile ad hoc networks (DSR). Internet draft. Draft-ietf-manet-dsr-08.txt.

[13] E.S. Babu and M.H.M.K. Prasad. 2013. An Implementation Analysis and Evaluation Study of DSR with Inactive DoS Attack in Mobile Ad hoc Networks. 2(6): 501-507.

[14] E.S. Babu, C. Nagaraju, and M.H.M.K. Prasad. 2013. An Implementation and Performance Evaluation of Passive DoS Attack on AODV Routing Protocol in Mobile Ad hoc Networks PROTOCOL OF. 2(4).