International Journal of Engineering Technology and Applied Science

(ISSN: 2395 3853), Vol. 2 Issue 10 October 2016

Mobile Ad - Hoc Network Detection and Prevention

[1]Sourabh Gangoli (M-Tech Scholar)
(Dept. of Information Science and Technology NRI IST, BHOPAL)
[1]Sourabh.ganguli@gmail.com
[2]Angad Singh
(Asst. Prof. Dept. of Information Science and Technology NRI IST, BHOPAL)

Abstract: Wireless mobile ad-hoc network (MANET) could also be a self-configuring network that consists of the many movable mobile nodes. These mobile nodes communicate with each other with none infrastructure. As wireless ad-hoc networks lack Associate in while not infrastructure, they are exposed to plenty of attacks.That the many researchers and authors of Ad-hoc network inside the past projected many solutions to form network safer and to produce further security to the users of purpose of read. One among these attacks is that the hollow attack. In this paper we have a tendency to tend to focuses our interest on wormhole attack, in wormhole attack Associate in MANET offender record packets at one location into the network, tunnel them to a distinct location and carry them there into the network. The wormhole attack is actually launched by a mix of collaborating nodes. In wormhole attack collaborating offender nodes occupy durable strategic locations in fully totally different components of the network. By occupying dominant positions in a {very} very network these nodes can cowl complete network and advertise to possess the shortest path for sending information. We have a tendency to tend to took AODV routing protocol for this analysis work and provide Associate in MANET economical answer to find and stop wormhole attack.

KEYWORD: AD-Hoc Network, MANET, Wireless Network.

1 Introduction: Wireless communications has emerged united of the foremost active space of technology development. The demand for additional wireless capability has fully grown at a very fast pace. Historically radio information measure and transmitter power area unit the resources that are wont to increase the capability of wireless systems. Sadly, these 2 resources area unit restricted within the preparation of wireless networks. These 2 resources don't seem to begrowing at rates that can support increasing demands for wireless capacity. On the other hand, another resource processing power is growing at a very rapid rate. Moore's Law which talks about doubling of processor capabilities in every 18 months has been quite accurate over the past 20 years. Increase in processor capability is promising new technologies and developments to fulfill increasing demands. Given these circumstances, developing new wireless capacity and the deployment of greater intelligence in Communication vary of host nodes should act as router and provides communication between all nodes. These nodes should communicate and get together with the users to forward knowledge packets to their final needed host. So each node acts each as a host and as a router. A mobile host is just a self-addressed IP host or entity. A router is ahost that is ready to run a routing protocol. So nodes within the ad hoc network perform routing to assist one another in relaying packets and construct a network themselves.

MOBILE AD-HOC NETWORK [MANET]

In recent years, the most of aim of ad hoc networks is to fulfill within the field of networking and wireless communication and. MANETs has become highly regarded. Ad hoc is comes from Latin word, "for this purpose" that means temporary. Mobile ad hoc Networks simple deployed mobile wireless network. Ad hoc networks by have several options which might facilitate to resolve some problems that is said to property between 2 devices. With the time of web digital communication between 2 hosts came into existence. However if we would like to use web connection between to hosts that are in immediate wireless continuously ought to use routers and switches at remote locations to forward packets among one another. Thanks to these options ad hoc networks have become a lot of helpful for applications such as: conferencing, emergency services for military and disaster management, detector networking, and intelligent transportation systems. Ad hoc networks may additionally be used in local area network, wide area network, campuses, companies and hospitals for connecting devices that are in range.

MANET could be a multi-hop, wireless network system created from a group of portable electronic equipment's with transmitter and receiver. This

cluster of mobile nodes could operate in remoteness, or could have gateways to interface with a fixed network. AN ad-hoc network not uses any centralized administration

AD HOC ON-DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

AODV could be a reactive routing protocol designed for ad hoc wireless networks. In AODV routes to attach 2 nodes are get only it's necessary i.e. on demand. AODV routing algorithmic rule is specially design for dynamic self-configured networks like MANET. AODV provides loop free routes alongside route management for broken links. Bandwidth need mobile nodes in AODV is relatively but different protocols as AODV doesn't need periodic route advertisements.

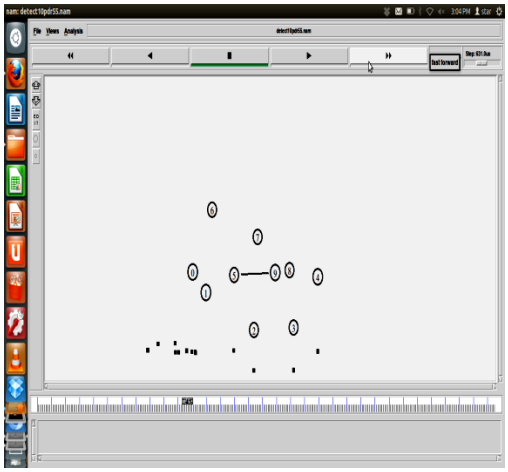
AODV uses symmetrical links between communication nodes. Nodes that are communicating nodes on active route solely keep routing data. Nodes that do lie on active path needn't maintain routing info and doesn't exchange routing table periodically. Moreover, routes are discovered and maintained between 2 nodes only they have to communicate or if they're acting because the intermediate node supporting in communication.

. **SIMULATION ENVIOURNMENT**

Simulation is that the replication of essential features of some system or method so as to study the characteristics or performance of the system. This thesis work requires a network simulator as the proposed work is based on MANET. There are many r 1.501360188 _2_ RTR --- 0 AODV 48 [0 ffffffff 0 800] ------- [0:255 -1:255 30 0] [0x2 1 1 [1 0] [0 4]]

SIMULATION TOPOLOGY

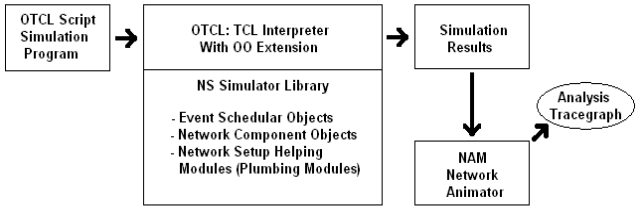
In this work, the simulation is configured with varying number of nodes starting from 5-node scenario up to 25-node scenario. Simulation is performed with both static and random movement of nodes



network simulators that can simulate the MANET routing protocols like OPNET, Glomo-Sim and NS-2 etc. In this work, Network Simulator (NS- 2) software version 2.34 (NS2.34) is used due to its open source simplicity and free availability.

NETWORK SIMULATOR

Network Simulator (NS) is a simulation tool developed and maintained by researchers at Berkeley. It is discrete event and object oriented simulator developed for networking research.



Tool command language

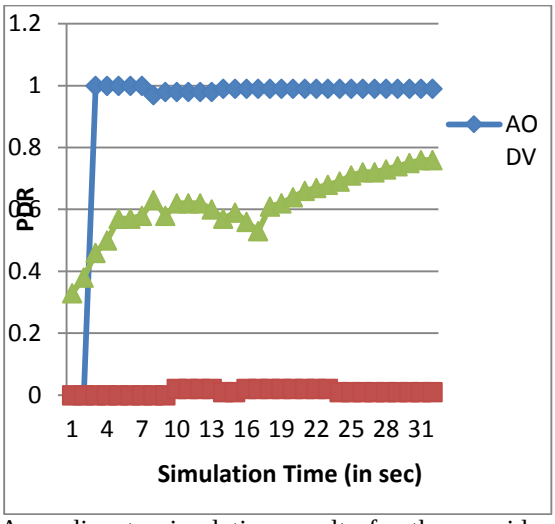
Tool command language (TCL) could be a scripting language wont to build the simulation scenario, traffic and node configuration for the system Trace File Analysis

NS-2 simulation generates results in the form of trace files. Trace file consists of complete data flow information of network. The traces in ns2 modify recording of information connected **with** packetevents like packet send, packet drop or arrival occurring in a queue or link. Example of wireless trace format for 'AODV' Ad-hoc network routing protocols:

RESULT ANALYSIS

The simulation results of AODV, wormhole AODV and MAODV routing protocols and their comparisons are shown in the following sub-section 5.3 in the form of graphs. The simulation analysis of three routing protocols primarily focuses on a few performance metrics discussed below

Simulation Results for 5-Nodes Scenario



According to simulation results for the considered 'network topology' of 5-nodes with regard to PDR, sender and therefore the receiver will transmit data directly or using one hop just in case of AODV routing protocol resulting in 100% PDR. Once AODV is simulated below wormhole attack the malicious node drops the packets transmission through them leading to poor PDR. However by using the planned technique to change AODV, PDR is accumulated on top of 70th even under wormhole attack. It also can be seen from the graph that with increase in simulation time, PDR improves for the planned technique.

- **Packet Delivery Ratio Comparison**

This subsection shows the packet delivery ratio of the three routing protocols, calculated for different number of nodes. The variation of packet delivery ratio with the number of nodes is shown in figure 5.21.

Table 5.2 PDR Comparison Chart of AODV, AODV under attack and modified AODV

No. of Nodes	AODV	AODV under wormhole attack	Modified AODV
5	99.4%	1.13%	76.8%
10	98.54%	1.46%	55.12%
15	98.66%	0.89%	47.32%
20	87.85%	0.81%	39.27%
25	86.97%	0.57%	42.21%

CONCLUSIONS

This paper applied the elaborate study and examination of AODV routing protocol and therefore the wormhole attack. In our work we proposed a method particularly hop-count analysis to spot the malicious nodes that causes wormhole tunnel. We had done Simulation of our projected answer within the presence of wormhole attack in numerous node and traffic situations. Simulation of security ways give the capability to pick out a decent security solution for routing protocols and provides the information the way to use this scheme in hostile and compromised environments. Consistent with simulation results our technique shows superior **performance as** PDR and turnout will increase but, "average end-to-end delay" additionally will increase. Within the analyzed situation, it's found that the MAODV features a superior performance then AODV. Changed AODV is appropriate for detection and prevention of wormhole attack. It improves the Packet delivery ratio under attack conditions, with a least decrease in turnout and acceptable increase in end-to-end delay.

Future Work

One of the leading problems in MANET communication is security. Security in MANET is compromised by some ways and attacks. Many different ways that to attack the networking that might be subject to more studies many different ways that also are offered to initiate a wormhole attack like packet leashing. So additional techniques are needed to notice them.Measurement of computing quality. Energy efficiency is additionally a really prime topic of concern for mobile nodes in MANET. As a result of they use batteries.

REFERENCES

[1] C.Siva Ram Murthy and B. S. Manoj. "Ad hoc wireless networks: Architecture and Protocols",PrenticeHall
Publishers, May 2004, ISBN 013147023X.
[2] P.V.Jani, "Security within Ad-Hoc Networks", Position Paper, PAMPAS Workshop, Sept. 16/17 2002.
[3] K. Biswas and Md. Liaqat Ali, "Security threats in Mobile Ad-Hoc Network", Master Thesis, Blekinge Institute of
Technology" Sweden, 22nd March 2007.
[4] Mishra Amitabh, Nadkarni Ketan M., and Ilyas Mohammad. "Security in wireless Ad-hoc networks, the handbook
of Ad hoc wireless network". Chapter 30: CRC PRESS Publisher, 2003.
[5] Roy, D.B., Chaki, R & Chaki, N. "A New Cluster-Based Wormhole Intrusion detection. Algorithm for Mobile Ad
Hoc Networks", International Journal of Network Security and its Applications (IJNSA), (2009).
[6] C.E.Perkins and E.M.Royer, "Ad-hoc On Demand Distance Vector Routing," Proceedings of the 2nd IEEE
Workshop on Mobile Computing Systems and Applictions, pp.90-100, Feb, 1999.
[7] C.M barushimana, A.Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in
Mobile Ad-Hoc Networks," Workshop on Advance Information Networking and Application, Vol. 2, pp. 679-
684, May, 2003.
[8] http://www.faqs.org/rfcs/rfc3561.html
[9] M.Abolhasan, T.Wysocki, E.Dutkiewicz, "A Review of Routing Protocols for Mobile Ad-hoc Networks,"
Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.
[10] http://www.netmeister.org/misc/zrp/zrp.html
[11] G. A. Pegueno and J. R. Rivera, "Extension to MAC 802.11 for Performance Improvement in MANETs",
Karlstads University, Sweden, December 2006.
[12] S. Lu, L. Li, K.Y. Lam, L. Jia, "SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.",
International Conference on Computational Intelligence and Security, 2009.
[13] C.Wei, L.Xiang, B.yuebin and G.Xiaopeng, "A New Solution for Resisting Gray Hole Attack in Mobile Ad-Hoc
Networks", Second International Conference on Communications and Networking in china, pp.366-370, Aug,
2007.
[14] Zhu, C. Lee, M.J.Saadawi, T., "RTT-Based Optimal Waiting time for Best Route Selection in Ad-Hoc Routing
Protocols", IEEE Military Communications Conference, Vol. 2, pp. 1054-1059, Oct, 2003.
[15] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for IsolatingSelfish nodes
in Ad-Hoc Networks," Second Annual International Conference on Mobile and Ubiquitous Systems, Networking
and Services, pp.3-11, July, 2005.
[16] [16] F.Stanjano, R.Anderson, "The Resurrecting Duckling: Security Issues for Ubiquitous Computing," Vol.35,
pp. 22-26, Apr, 2002.
[17] [17] H.L.Nguyen,U.T.Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks,"
International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006.
[18] [18] Y.-C. Hu, A. Perrig, D. B. Johnson; "Packet leashes: a defense against wormhole attacks in wireless
networks"; INFOCOM 2003, Twenty-Second Annual Joint Conference of the IEEE Computer and Communication
Societies, Vol. 3, pp. 1976-1986, 2003.
[19] [19] S.Capkun, L. Buttyan, J.-P. Hubaux; "SECTOR: Secure Tracking of Node Encounters in Multi-Hop Wireless
Networks"; Proc. of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks; 2003.