ISSN No. 0976-5697

Volume 4, No. 6, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

A Survey On New Approach For Detecting Blackhole Attack

Ankush D. Patil
Computer Science &Engineering Department,
SIRT, Bhopal, India
ankushpatil48@gmail.com

Jyoti B. Rathi
Computer Science &Engineering Department,
JDIET Yavatmal, India
jyoti.rathi08@gmail.com

Yogadhar Pandey
Computer Science &Engineering Department,
SIRT, Bhopal, India
p_yogdhar@yahoo.co.in

Abstract: Security is an essential requirement in mobile ad hoc networks to provide protected communication between mobile nodes. A MANET is a self-organizing system of mobile nodes that communicate with each other via wireless links with no .fixed infrastructure or centralized administration such as base stations or access points. Due to unique characteristics of MANETS, it creates a number of consequential challenges to its security design. To overcome the challenges, there is a need to build a security solution that achieves both broad protection and desirable network performance. MANETs are vulnerable to various attacks, such as blackhole attack, jellyfish attack, rushing attack, wormhole attack. Black hole is a type of routing attack where a malicious node advertise itself as having the shortest path to all nodes in the environment by sending fake route reply. By doing this, the malicious node can deprive the traffic from the source node. Although in this paper we only focus on the routing protocols and security issues in MANET. In this paper, we proposed an AODV and DPRAODV (Detection, Prevention and Reactive AODV) to prevent security threats of blackhole by notifying other nodes in the network of the incident.

Keywords: AODV, Blackhole attack, MANETs, Routing protocol**,**

I. INTRODUCTION

In this era of wireless devices, Mobile Ad-hoc Network (MANET) has become an indivisible part for communication for mobile devices. Therefore, interest in research of Mobile Ad-hoc network has been growing since last few years. Mobile Ad-hoc Network (MANET) is a collection of wireless mobile hosts without fixed network infrastructure and centralized administration (Fig-1).

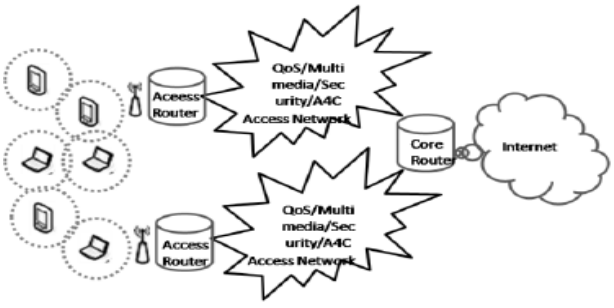

Figure-1 Mobile Ad-hoc Network

Communication in MANET is done via multi-hop paths. Lots of challenges are there in this area: MANET contains diverse resources; the line of defense is very ambiguous; Nodes operate in shared wireless medium; Network topology changes unpredictably and very dynamically; Radio link reliability is an issue; connection breaks are pretty frequent. Moreover, density of nodes, number of nodes and mobility of these hosts may vary in different applications. There is no stationary infrastructure. Each node in MANET acts a router that forwards data packets to other nodes. Therefore, selection of effective, suitable, adaptive and robust routing protocol is of utmost importance.

Mobile ad hoc network (MANET) is one of the recent active fields and has received spectacular consideration because of their self-configuration and self-maintenance. But security has become primary concern to provide protected communication between mobile nodes in a hostile environment. Although mobile ad hoc networks have several advantages over wired networks, on the other side they pose a number of non-trivial challenges to the security design as they are more vulnerable than wired networks. In this paper, we have considered a fundamental security problem in MANET to protect its basic functionality to deliver data bits from one node to another. Nodes help each other in conveying information to and fro and thereby creating a virtual set of connections between each other. Routing protocols play an imperative role in the creation and maintenance of these connections. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is a blurry boundary separating the inside network from the outside world.

a. Routing protocol:

Many different types of routing protocols have been developed for ad hoc networks by Royer and Toh (1999). There are three types of routing protocols: Proactive (periodic) Protocols, Reactive (on-demand) Protocols and Hybrid Protocols.

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

Proactive protocols are table-driven that constantly update lists of destinations and routes. Reactive protocols respond on demand. Hybrid protocols combine the features of reactive and proactive protocols. In a proactive routing protocol, nodes periodically exchange routing information with other nodes in an attempt to have each node always know a current route to all destinations. In a reactive protocol, on the other hand, nodes exchange routing information only when needed, with a node attempting to discover a route to some destination only when it has a packet to send to that destination. The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency.

A. Attacks on MANET:

Wireless ad hoc networks are vulnerable to various attacks. These include wormhole attack, black hole attack, flooding attack, packet dropping attack, route disruption attack active interfering, impersonation, and denial-of-service. Attacks on MANETs can be categorized in several ways. One method of characterization is to distinguish them according to their objective: Denial-of-Service (D o S) attacks for example try to disturb normal network and/or node operation while others attempt to completely terminate all activity (e.g. black hole and flooding attacks).Still other attack mechanisms aim to garner a more powerful position in the network by manipulating routing packets (e.g. wormhole attacks) which allows attackers to eavesdrop and manipulate packets (e.g. to break confidentiality and integrity).

a. Black Hole Attack: The black hole attack generates and disseminates incorrect routing information so that packets are no longer forwarded to the intended recipient; instead they are lost or forwarded to an attacking node. Fig. 2 shows an example of normal data traffic transferred via adjacent nodes to node D on the left and the effects of a successful attack on the right. Messages intended for node D do not reach their desired target but are instead intercepted by the attacking node.

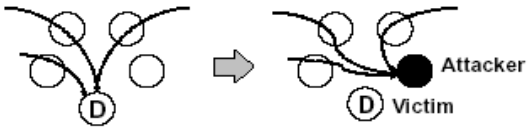

Figure 2. Data flow to target D before and during a black hole attack

b. Wormhole Attack: A wormhole attack uses two cooperating corrupted nodes of a network connected by an out-of-band channel to re-route data traffic. Attackers use wormholes in the network to make their nodes appear more attractive (with perceived faster transfer times) so that more data is routed through their nodes.

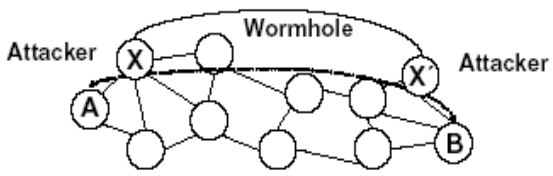

Figure 3. Data flow during a wormhole attack of X and X′

c. Flooding Attack: Flooding attacks have the dangerous characteristic that they are simple to implement but may cause high damage. An attacker can create and send messages with varying destination addresses, varying content.
d. Packet Dropping Attack: A packet dropping attacker discards all or a fraction of received messages. Alternatively attackers may also discard all or a percentage of messages, the latter having the advantage to be more difficult to detect as there is no permanent influence on the network.
e. Route Disruption Attack: This type of attack attempts to disrupt MANET routing processes by sending manipulated routing messages that include source and/or destination nodes that do not exist in the MANET.

A single solution cannot resolve all the different types of attacks in ad hoc networks. In this paper, we have designed a novel method to detect black hole attack: DPRAODV, which isolates that malicious node from the network. We have complemented the reactive system on every node on the network. This agent stores the Destination sequence number of incoming route reply packets (RREPs) in the routing table and calculates the threshold value to evaluate the dynamic training data in every time interval as in.

Our solution makes the participating nodes realize that, one of their neighbors is malicious; the node thereafter is not allowed to participate in packet forwarding operation. In Section 2 of this paper, we summarize the basic operation of AODV (Ad hoc On-Demand distance Vector Routing) protocol on which we base our work. In Section 3, we discuss related work. In Section 4, we describe the effect of black hole attack in AODV. Section 5 presents the design of our protocol; DPRAODV that protects against black hole attack. Section 6 presents conclusion.

II. BACKGROUND OF AODV

AODV is a reactive routing protocol; that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further, the nodes do not have to discover and maintain a route to another node until the two needs to communicate, unless former node is offering its services as an intermediate forwarding station to maintain connectivity between other nodes. Whenever a source node needs to communicate with another node for which it has no routing information, Route Discovery process is initiated by broadcasting a Route Request (RREQ) packet to its neighbors. Each neighboring node either responds the RREQ by sending a Route Reply (RREP) back to the source node or rebroadcasts the RREQ to its own neighbors after increasing the hop-count field. If a node cannot respond by RREP, it keeps track of the routing information in order to implement the reverse path setup or forward path setup. The destination sequence number specifies the freshness of a route to the destination before it can be accepted by the source node. Eventually, a RREQ will arrive to node that possesses a fresh route to the destination. If the intermediate node has a route entry for the desired destination, it determines whether the route is fresh by comparing the destination sequence number in its route table

entry with the destination sequence number in the RREQ received.

If a node receives more than one RREPs, it updates its routing information and propagates the RREP only if RREP contains either a greater destination sequence number than the previous RREP, or same destination sequence number with a smaller hop count. It restrains all other RREPs it receives. The source node starts the data transmission as soon as it receives the first RREP, and then later updates its routing information of better route to the destination node. Each route table entry contains the following information:

a. Destination node
b. Next hop
c. Number of hops
d. Destination sequence number
e. Active neighbors for the route
f. Expiration timer for the route table entry

As the link is broken and node receives a notification, and Route Error (RERR) control packet is being sent to all the nodes that uses this broken link for further communication. And then, the source node restarts the discovery process. As the routing protocols typically assume that all nodes are cooperative in the coordination process, malicious attackers can easily disrupt network operations by violating protocol specification. This paper discusses about black hole attack and provides routing security in AODV by purging the threat of black hole attacks.

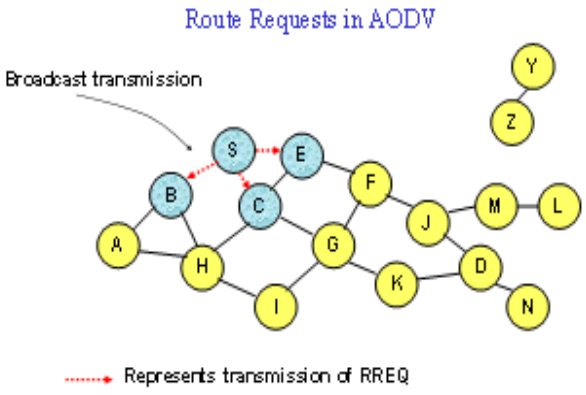

Figure 4a.Route request in AODV

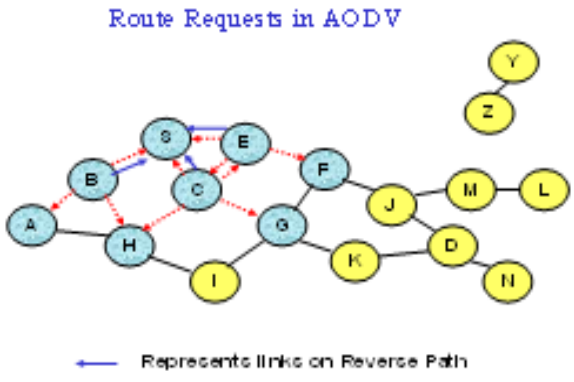

Figure 4b.Route request in AODV

III. SECURING AODV

There are basically two approaches to secure MANET:

a. Securing Ad hoc Routing and
b. Intrusion Detection

A. Secure Routing:

The Secure Efficient Ad hoc Distance vector routing protocol (SEAD) employs the use of hash chains to authenticate hop counts and sequence numbers in DSDV. Another secure routing protocol, Ariadne assumes the existence of a shared secret key between two nodes based on DSR (reactive) routing protocol. The computation overhead involved in the above mentioned protocols is awful and often suffer from scalability problems. As a preventive measure, the packets are carefully signed, but an attacker can simply drop the packet passing through it, therefore, secure routing cannot resist such internal attacks. So our solution provides a reactive scheme that triggers an action to protect the network from future attacks launched by this malicious node.

B. Intrusion Detection System:

Zhang and Lee present an intrusion detection technique for wireless ad hoc networks that uses cooperative statistical anomaly detection techniques. The use of anomaly based detection techniques results in too many number of false positives. Stamouli proposes architecture for Real-Time Intrusion Detection for Ad hoc Networks (RIDAN) .The detection process relies on a state-based misuse detection system. Therefore, each node requires extra processing power and sensing capabilities. In the method requires the intermediate node to send Route Confirmation Request (CREQ) to next hop towards the destination. This operation can increase the routing overhead resulting in performance degradation. Therefore, a method that can prevent the attack without increasing routing overhead and delay is required all the above mentioned approaches except, use static value for threshold. To resolve the problem, threshold value should be reflecting current network environment by updating its value. And also, our solution ensures that a node once detected as malicious cannot participate in forwarding and sending of a data packet in the network.

IV. DESCRIPTION OF BLACK HOLE ATTACK

MANETs are vulnerable to various attacks. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad hoc network. Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages; such as sequence number and hop count. A basic attack that an adversary can execute is to stop forwarding the data packets. As a result, when the adversary is selected as a route, it denies the communication to take place.

Black hole attacks: A black hole is a malicious node that falsely replies for route requests without having an active route to the destination. It exploits the routing protocol to advertise itself as having a good and valid path to a destination node. It tries to become an element of an active route, if there is a

chance. It has bad intention of disrupting data packets being sent to the destination node or obstructing the route discovery process. Cooperative black hole attack is caused by many neighbor black holes co operating each other. Black hole attack may be internal or external. In black hole attack, the malicious node waits for the neighbors to initiate a RREQ packet. As the node receives the RREQ packet, it will immediately send a false RREP packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a black hole as it swallows all objects; data packets.

Fig. 5 shows an example of normal data traffic transferred via adjacent nodes to node D on the left and the effects of a successful attack on the right. Messages intended for node D do not reach their desired target but are instead intercepted by the attacking node.

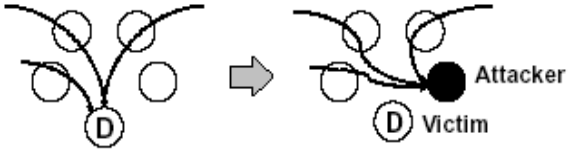

Figure 5: Data flow to target D before and during a black hole attack

In figure 6, source node S wants to send data packets to a destination node D in the network. Node M is a malicious node which acts as a black hole. The attacker replies with false reply RREP having higher modified sequence number. So, data communication initiates from S towards M instead of D.

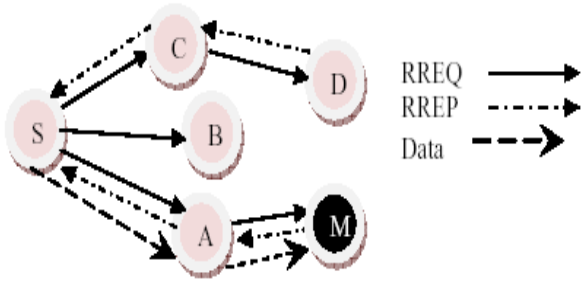

Figure 6. Black hole attack in MANET

V. DPRAODV: SOLUTION AGAINST BLACK HOLE ATTACK

In an implementation using AODV an attacker may distribute manipulated Route Reply (RREP) messages in order to be included in many valid network routes and to appear as an attractive relay for as many target nodes as possible. When the attacker receives a Route Request (RREQ) message it creates and sends a manipulated RREP message indicating a shorter transport distance through that node. Attackers also have the option of manipulating only a fraction of RREP messages to reduce probability of detection. Hop counts of manipulated RREP messages are decreased in order to purport to have shorter routes to the destination node. Sequence numbers are also increased to make messages appear newer and thus increase the probability that the sending node will accept them. In normal AODV, the node that receives the RREP packet first checks the value of sequence number in its routing table. The RREP packet is accepted if it has REP_seq_no higher than the one in routing table. Our solution does an addition check to find whether the RREP_seq_no is higher than the threshold value. The threshold value is dynamically updated as in every time interval. As the value of RREP_seq_no is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbors.

The ALARM packet has the black list node as a parameter so that, the neighboring nodes know that RREP packet from the node is to be discarded. Further, if any node receives the RREP packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. It simply ignores the node and does not receive reply from that node again. So, in this way, the malicious node isolated from the network by the ALARM packet. The continuous replies from the malicious node are blocked, which results in less Routing overhead.

Moreover, unlike AODV, if the node is found to be malicious, the routing table for that node is not updated, nor the packet is forwarded to another node. The threshold value is dynamically updated using the data collected in the time interval. If the initial training data were used, then the system could not adapt the changing environment. The threshold value is the average of the difference of dest_seq_no in each time slot between the sequence number in the routing table and the RREP packet. The time interval to update the threshold value is as soon as a newer node receives a RREP packet.

As a new node receives a RREP for the first time, it gets the updated value of the threshold. So our design not only detects the black hole attack, but tries to prevent it further, by updating threshold which reflects the real changing environment. Other nodes are also updated about the malicious act by an ALARM packet, and they react to it by isolating the malicious node from network.

VI. CONCLUSION

MANETs are vulnerable to various attacks. A basic attack that an adversary can execute is to stop forwarding the data packets. AODV is a reactive routing protocol; that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further, the nodes do not have to discover and maintain a route to another node until the two needs to communicate, unless former node is offering its services as an intermediate forwarding station to maintain connectivity between other nodes.

In DPRAODV (Detection, Prevention, Reactive AODV), we have used a very simple and effective way of providing security in AODV against black hole attack. Our prevention scheme detects the malicious nodes and isolates it from the active data forwarding and routing and reacts by sending ALARM packet to its neighbors.

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India

VII. REFERENCES

[1] Hao Yang, Haiyun Luo. Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: Challenges and solutions". IEEE Wireless Communications, February 2004

[2] Shree, Murthy and J. J. Garcia-Luna-Aceves. "An Efficientrouting Protocol for Wireless Networks". MobileNetworks and Applications, 1(2):183–197, 1996.

[3] Charles E.Perkins and Elizabeth M. Royer. "Ad-Hoc on-DemandDistance Vector Routing". In Proceedings of theSecond IEEE Workshop on Mobile Computing Systems andApplications (WMCSA'99), pages 90–100, February 1999.

[4] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kat, AbbasJamalipour, and Yoshiaki Nemoto, "Detecting BlackholeAttack on AODV-based Mobile Ad Hoc Networks byDynamic Learning Method", International Journal ofNetwork Security, Vol.5, No.3, P.P 338-346, Nov. 2007

[5] C. Perkins and P. Bhagwat. "Routing over multihop wireless Network for mobile computers". SIGCOMM '94: ComputerCommunications Review:234-244, Oct. 1994.

[6] C. E. Perkins, S.R. Das, and E. Royer, "Ad-hoc on Demand Distance Vector (AODV)". March 2000,http://www.ietf.org/internal-drafts/draft-ietf-manet-aodv-05.txt

[7] Ioanna Stamouli, "Real-time Intrusion Detection for Ad hoc Networks" Master's thesis, University of Dublin,September 2003.

[8] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: SecureEfficient Distance Vector Routing for Mobile Wireless Adhoc Networks," Proc. 4th IEEE Workshop on MobileComputing Systems and Applications, Callicoon, NY, June2002, pp. 3-13.

[9] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A SecureOn-Demand Routing Protocol for Ad hoc Networks," Proc.8th ACM Int'l. Conf. Mobile Computing and Networking(Mobicom'02), Atlanta, Georgia, September 2002, pp. 12-23.

[10] Kimaya Sanzgiti, Bridget Dahill, Brian Neil Levine, Clayshields, Elizabeth M, Belding-Royer, "A secure RoutingProtocol for Ad hoc networks In Proceedings of the 10thIEEE International Conference on Network Protocols (ICNP' 02), 2002

[11] S. Yi, P. Naldurg, and R. Kravets, "Security-Aware Ad hoc Routing for Wireless Networks," Proc. 2nd ACM Symp.Mobile Ad hoc Networking and Computing (Mobihoc'01),Long Beach, CA, October 2001, pp. 299-302.

[12] Y. Zhang and W. Lee, "Intrusion detection in wireless ad – hoc networks," 6th annual international Mobile computingand networking Conference Proceedings, 2000.

[13] S. Lee, B. Han, and M. Shin, "Robust routing in wireless adhoc networks," in ICPP Workshops, pp. 73, 2002.

[14] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attackin wireless ad hoc networks," in ACM 42nd SoutheastConference (ACMSE'04), pp. 96-97, Apr. 2004.

[15] Dokure, Semih." Simulation of Black hole attack inwirelessAd-hoc networks". Master's thesis, AtýlýmUniversity,September 2006

[16] Kevin Fall and Kannan Varadhan (Eds.), "The ns Manual", 2006, available from http://www-mash.cs.berkeley.edu/ns/

CONFERENCE PAPER
"A National Level Conference on Recent Trends in Information Technology and Technical Symposium" On 09th March 2013
Organized by
Dept. of IT, Jawaharlal Darda Inst. Of Eng. & Tech., Yavatmal (MS), India