IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Performance Enhancement of AODV in MANET over Black-Hole Attack

Mr. Ankush Jain[1], Mr. Sandeep Gupta[2]

Department of Electronics & Communication, SD Bansal College of Technology, Indore[1,2]

Abstract: A blackhole attack is the most emerging security threat in ad-hoc network. Here, malicious node attempt to compromise mobile nodes and drop packet respectively. Blackhole attack may apply through internal or external mode either to disrupt the communication or degrade network performance by dropping the packet. Here, malicious node attempt to get benefitery position into network to compromise the victim node. In Blackhole attack, malicious node attempt to get achievable position into network and start dropping packets respectively. Work observes that all it happened due to weakness of AODV routing protocol. This research work attempts to develop a mitigation algorithm to avoid and prevent genuine nodes from malicious attack. The complete research work is classified into three categories which are without attack, with attack and preventive scenario. Various scenarios based on variable mobile nodes, speed, pause time and area has been configured to observe the impact of blackhole attack and proposed mechanism with different situation. A NS2 simulator has been used to simulate and evaluate the performance of proposed solution. The complete experimental setup concludes that improvement in mobile node increase the network performance but also increase the blackhole impact. Subsequently, improvement in node speed degrades the blackhole impact. The complete work conclude with the fact the performance of modified AODV is similar with traditional AODV routing protocol but give great height in respect to blackhole attack.

Keywords: AODV, MANET, Black-Hole, Ad-hoc.

INTRODUCTION

A MANET is known as mobile ad-hoc networks collection of mobile nodes without having any infrastructure or central control. It is characterized by ad-hoc due to dynamic nature of network topology and node specification. Here, node may leave and join the network with wireless communication media as per application requirement.

Challenges in such networks is to protect the network from attackers who can attack on network and have unauthorized access to all information, may theft the private data and use it in unethical manner or may forge someone identity. On-demand routing protocol has a route discovery process initiated by sender.

When a traffic resource needs a route, it initiates a RDP (route discovery process) by sending a route request for the destination (typically via a network-on wide flood) and waits for a route reply.

There are various kind of routing protocols are proposed and developed to discover route in dynamic topology based network. On-demand routing protocols may be single path or multipath protocols find various routes from source to destination. Here, Source node advertises the route discovery packet to establish route between sender and receiver. It also uses route repairing mechanism to recover damage routes.

The major challenge with AODV routing protocols are they don't have any security policy to detect and avoid security attack.

Proposed work focus on to avoid security attack and prevent network from attackers attempt.

Advantages of Mobile Ad-Hoc Network:

The advantages of a mobile Ad-Hoc network include the following-

1. Independent and decentralize control.
2. Self configurable network.
3. Each node may act as simple node and router.
4. Less expensive in the comparison of wired network.
5. Scalable and flexible network due to mobility factor.
6. Very robust and useful network.

RELATED WORK

Various other approaches are proposed in the last few years based on existing mechanism like a watchdog in As the main advantage of it is that the watchdog only needs local information and, therefore, it becomes quite difficult for it to be badly influenced by another node. But it has two disadvantages

1. The watchdog is vulnerable to cooperative attacks, and
2. It is not so accurate when we increase node's mobility.

It also proposes an improvement in this mechanism which can be used in MANET. The watchdog is a basic module for several different IDS, making an extra effort for improving it becomes a necessity. The proposed improvements can cope up well with the watchdog weaknesses based on Kalman filters. We propose a technique similar to the one used in SPAM filters used for emails: Kalman filters which is better than optimized Bayesian filter additionally, to avoid collaborative attacks; we propose an information exchange strategy similar to a voting system. In the previous section we showed how mobility affects the capacity of the watchdog for detecting

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

an attacker. In the literature we can find a reliable and extensive set of tools for detecting abnormal behaviors considered malicious in other fields, such as the SPAM filters. A SPAM filter can segregate illegitimate spam email from legitimate email. This email filters are normally based on basic Bayesian filters, which allow the mail client to learn about the user decisions. Basic Bayesian filters are not only useful for detecting SPAM.[6]

Another improvement of the approach is avoidance of collaborative black-hole attack. A secure exchange of information among nodes allows determining whether if a node is acting as an accomplice, and also marks it as being malicious.

In the current paper [7], a comparison is made between various existing IDS based on inputs, outputs, processes, benefits and drops. After studying the various approaches and their benefits the paper also suggested some guidelines for selecting effective IDS for larger security. In this section, some guidelines are developed to assist selecting intrusion detection methods in MANET. Guideline 1: In MANET which requires a high detection rate and low false alarm rate And have abundant network resources and computational resources at each node, the IDS should use data mining or neural network as the local detection techniques in each node and use collaborative decision making between nodes. Guideline 2: In MANET where the network resources are limited and security requirement for IDS is not high, mobile agent should be used as the communication mechanism between nodes. Guideline 3: For IDS whose scalability and security requirements are not high, mobile agent should be used to conduct detection on each node. Guideline 4: For IDS which can be expanded to work with multiple types of audit data, and security requirement for IDS. The paper also performs few experiments to prove the comparison results and will direct the further researches. The paper also presents a case study of an MIS/CIS/CS curriculum on the first introduction of the new technology for IDS in MANET. Similarly, carrying forward the above research concern a comparative study is developed to analyze the IDS architectures proposed in the existing literatures [8].

AD-HOC ON DEMAND ROUTING PROTOCOL (AODV)

To understand the problem of black hole attack on AODV routing protocol first we understand the some common characteristics and it's working of AODV routing protocol in mobile environment. After that we take a look of the black hole attack, attacking mechanism in the AODV routing protocol. Ad-hoc on-demand distance vector (AODV) routing protocol uses an on demand approach for finding routes for communication such a route is established only when it is required by a source node for transmitting a data packet. It allows all mobile nodes, to pass messages through their neighbors to the node which are not in radio frequency range for communication. AODV protocol does this by discovering the routes along which message and information can be send. AODV protocol take precaution for such routes that they do not contain loops and tries to find the shortest route possible. AODV is also able to handle changes in route and can create new routes if there is an error. AODV defines three types of control message for route maintenance:

There are three types of control messages in AODV which are discussed below.

1. Route Discovery
2. Route Reply (RREP)
3. Route Maintenance

RREQ- When one node needs to send a message to another node that is not its neighbor it broadcasts a Route Request (RREQ) message.

RREP- A route reply message is unicast back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a correct route to this address.

RERR- Node monitors the link status of next hops in active routes and when a connection breakage in an active route is detected, a RERR message can be used to notify to the other nodes of the loss of the link.AODV uses sequence numbers to ensure loop freedom.

BLACK-HOLE ATTACK

In this attack a malicious node advertises itself as having the shortest path to other nodes of the network. Nevertheless, as soon as it receives packets destined for other nodes, it drops them instead of forwarding to the final destination. In our simulation scenario, each time a malicious black hole node receives a Route Request packet; it sends a Route Reply packet to the destination without checking if it really has a path towards the selected destination. Thus, the black-hole node is always the first node that responds to a Route Request packet. Moreover, the malicious node drops all Route Reply and Data packets it receives if the packets are destined to other nodes.

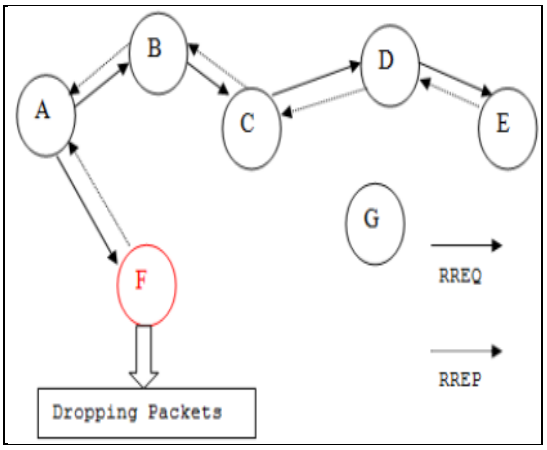

Figure: Security Attack on Mobile Ad-hoc Network

Black-hole Techniques

1. Highest Sequence Number with Min. Hop Count
2. Route Table Modification (Update Wrong Route Message)
3. Wired Connection

DOI 10.17148/IJARCCE.2016.52102

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

4. Adapting techniques of other Security Threats i.e. Wormhole Attack

PROBLEM DEFINITION

The AODV routing protocol is a popular reactive routing protocol in wireless networks. AODV is the successor of Distance Vector routing protocol developed with aim to enhance the performance of ad-hoc network. AODV routing protocol designed for better performance of the network not for security of node. Secure protocols are generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. For security purpose AODV have vulnerabilities and it is easily manipulate by malicious node to destroy its network routing.

The open nature of wireless medium also makes it easy for outsider attackers to interfere and interrupt the legitimate traffic. This concept classifies the attacks into two broad categories, namely Passive and Active attacks. In Passive attack, the adversary only eavesdrop upon the packets content, while packets may get dropped or altered on way in case of Active attacks. One of the widely known attacks is the Blackhole Attack. It is the variation of Worm- hole attack. Worm-hole attack is one of the security threat in which the traffic is redirected to such a node that actually does not exist in the network and that node drops the entire packet. The complete study observes that, AODV is a insecure routing protocol and does not incorporate any mechanism to detect and prevent communication from malicious affect.

The main purposes are following as:

1. Analyze and simulate the AODV protocol in MANET.
2. Analyze and simulate the impact of Black-hole attack on AODV in detail for various scenarios.
3. Propose a technique for detection of malicious node under Black-hole attack in AODV.
4. Propose a technique for prevention of malicious node under Black-hole attack in AODV and analyze its performance.
5. Simulate and analyze its performance of modified AODV and compare with the normal AODV.

SOLUTION DOMAIN

In this section the proposed mechanism for defending against black hole attack is presented. The mechanism modifies the AODV protocol by introducing three concepts,

- ✓ Broadcast Hello packet,
- ✓ Suspicious Node Detection
- ✓ Suspicious Node Prevention

A. Broadcast Hello packet

This research work proposes the blackhole detection for AODV by verifying the Hello packets. The Hello packets are normally broadcast to the source node by any intermediate node having the route to the destination. In order to detect blackhole attack, Hello packets are monitored. In the proposed modification of AODV routing protocol the Hello sent by intermediate nodes or the destination node is broadcasted.

B. Suspicious Node Detection

In the proposed scheme, each and every node receives broadcasted hello packet and process the capability check of every mobile node. Here, Hello packet consist the detection mechanism with collect the hardware information of current node and verify with threshold value. If any node observe with extra ordinary capability it consider as the malicious node and forward to prevention mechanism

C. Suspicious Node Prevention

The proposed scheme relies on detection mechanism integrated into hello packet. Here , It receive the malicious node information from blackhole detection mechanism and forward to shutdown. This mechanism intentionally shutdown the malicious node to prevent the genuine communication and intentional packet drop. This mechanism not only shutdown the malicious node but also improve the network performance during blackhole condition.

Simulation of Mobile Ad-hoc Networks.

The complete work has been classified into three different situations which are listed below:

1. Simulation and Performance observation of MANET with Normal condition
2. Simulation and Performance observation of MANET with Blackhole Attack
3. Simulation and Performance observation of MANET with proposed Detection & Prevention Technique

RESULT OBSERVATIONS

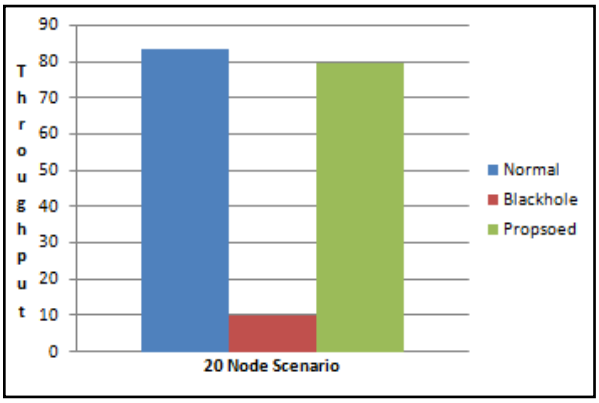

Figure 1: Comparison of Throughput

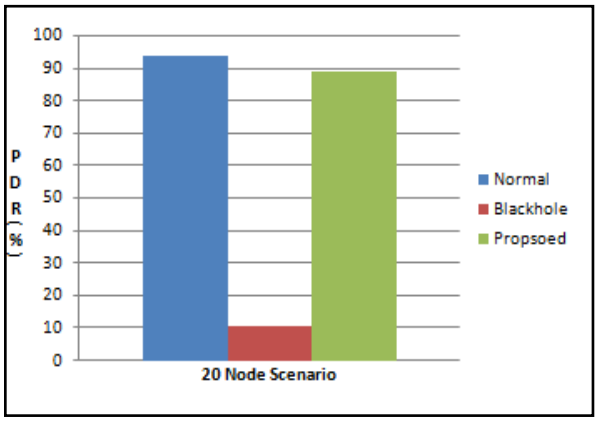

Figure 2: Comparison of PDR

DOI 10.17148/IJARCCE.2016.52102

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

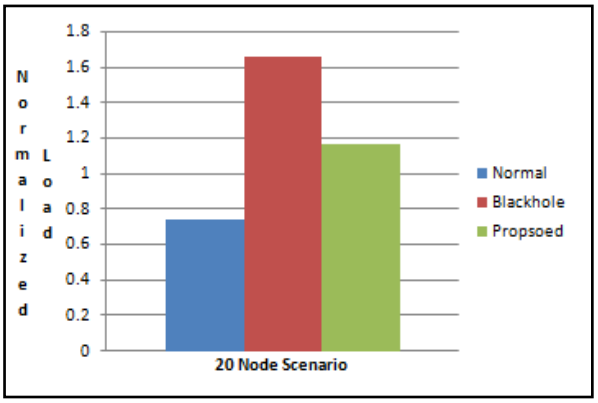

Figure 3: Comparison of E2E Delay

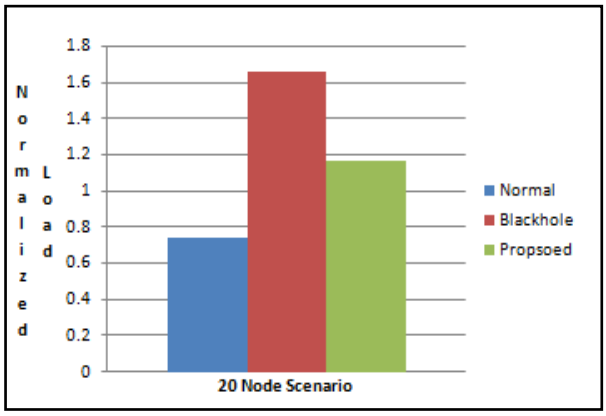

Figure 4: Comparison of Normalized Load

This section consist the performance observation of AODV routing protocol against variable mobile nodes into network. Figure 1, 2, 3 & 4 shows that improvement in mobile nodes increases the possibility of intermediate node between source and destination. This section comprises the results of variable mobile nodes with constant area, speed and pause time. The complete simulation observes that increment in number of mobile nodes increases the throughput and packet delivery ratio with respect to enhancement. Subsequently, it increases the impact of blackhole node with respect to node enhancement. It is also observe that End-to-End delay and Normalized Load degraded with respect to scaling. A similar result has been observed between normal AODV and modified preventive AODV. Furthermore, a wide gap has been observed in between Blackhole AODV and normal AODV. The complete simulation concludes that increment in mobile nodes increase the network performance and security factor.

CONCLUSION

The complete work concludes that proposed solution successfully detect and mitigate the blackhole attack in MANET. It is also observe that proposed algorithm help to improve the network performance during attacking situation.

REFERENCES

1. Mohamad Y. and Alsaadi, Yi Qian "Performance Study of a Secure Routing Protocol in Wireless Mobile Ad Hoc Networks" published in proceeding of 2nd International Symposium on Wireless Pervasive Computing, 5-7 Feb. 2007, pp 425-430.'
2. Li Zhitang and Shi Shudong " Secure Routing Protocol for Mobile Ad hoc Networks" published in proceeding of 6th IEEE/ACIS International Conference on Computer and Information Science (ICIS 2007)
3. Nisha P John and Ashly Thomas " Prevention and Detection of Black Hole Attack in AODV based Mobile Ad-hoc Networks - A Review" published in proceeding of International Journal of Scientific and Research Publications, Volume 2, Issue 9, September 2012
4. Yanzhi Ren, Mooi Choo Chuah, Jie Yang, Yingying Chen "Detecting Blackhole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording" available on IEEE Xplorer 2007.
5. Irshad Ullah & Shoaib ur Rehman " Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols" Master of Science, School of Computing - Blekinge Institute of Technology, Ronneby, Sweden
6. Sagar Pandiya, Rakesh Pandit and Sachin Patel, "Survey of Innovated Techniques to Detect Selfish Nodes in MANET", in International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), ISSN 2250-1568, Vol. 3, Issue 1, Mar 2013, 221-230.
7. S. P. Manikandan and Dr. R. Manimegalai, "Evaluation of Intrusion Detection Algorithms for Interoperability Gateways in Ad Hoc Networks", in International Journal on Computer Science and Engineering (IJCSE), ISSN: 0975-3397 Vol. 3 No. 9 September 2011.
8. Tushar Sharma, MayankTiwari, Prateek Kumar Sharma, Manish Swaroop and Pankaj Sharma, "An Improved Watchdog Intrusion Detection Systems In Manet", in International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 2 Issue 3, March-2013.