Implementing and Comparing LIDBPP (Local Intrusion Detection by Bluff Probe Packet)

[1]Imad I. Saada, [2]Majdi Z. Rashad, [3]Rasha H. Sakr

[1,2,3]Department of Computer Science, Faculty of Computers and Information Mansoura University, Egypt

Abstract

MANET (Mobile ad hoc network) is wireless network, it has a group of nodes which are communicating without any infrastructure. The security of MANET has been a desirable researching point. One of the well known threats in MANET is the black hole threat. Many approaches have been featured to bypass this kind of threats. However, these solutions do not prevent or avoid the threat totally, and in different degrees they affect the performance of MANET negatively.

This paper will implement a new approach named the Local Intrusion Detection by Bluff Probe Packet (LIDBPP) which was proposed in order to solve the black hole problem. The bluff Packet which contains virtual destination address has been created to trick the black hole. This new approach adopts a novel strategy for the detection of multiple black hole attacks with a minimum negative effect on the performance of the network. The algorithm has been simulated using NS2 simulator to examine the ability of the proposed LIDBPP approach to block the black hole attack, the simulation is also used to measure how much this approach may influence the network performance. The simulation results show that LIDBPP prevents the collaborative black hole attacks with less negative impact on the performance of MANET, so that it was very close to the performance of MANET without assumed black holes, and the simulation also is done to compare the performance of MANET in case of LIDBPP and in case of MAODV (Detection using negotiation with neighbors), the simulation proves that the performance of the network is slightly better with existence of LIDBPP.

Key Words:

MANET, Black Hole, Network Security, LIDBPP, AODV

1. Introduction

Security threat in MANET causes a big security challenge if it is compared to another kinds of wired or wireless networks because of several reasons such as:

The frequent moving of the nodes.

The lack of infrastructure.

The wireless connection.

Some researchers have partially succeeded in preventing the threats, the success of any approach is represented by preventing the threats and by reducing the negative effects on the performance of MANET. The main interest in this paper is to implement a novel solution called Local Intrusion Detection by Bluff Probe Packet (LIDBPP), and to study it experimentally. The strategy of LIDBPP is based on creating bluff message (message with virtual address).

The remaining sections of the research are organized as follow: in section 1.1, an overview of the reactive routing approach (AODV) is presented. Then, the research involves discussion of the black hole threat in section 1.2. Section 2 involves some of the existing solutions for the malicious node in MANET. Section 3 has a discussion of LIDBPP solution, section 4 contains the simulation of the implemented algorithm using NS2 and the results are discussed. Finally, the conclusions the future work were discussed in section 5.

1.1 Overview of AODV Routing Protocol

The most popular reactive routing protocol is the On-Demand Distance Vector routing protocol (AODV), the paper cares about AODV routing protocol because LIDBPP is implemented on AODV based MANET.

AODV is considered as a reactive routing protocol, by this routing protocol the routing information is saved in each nodes. AODV protocol initiates the discovery process just when it is needed by broadcasting the discovery packets these packets are called route request messages (RREQ), when the node receives RREQ, and if it has a route to the destination it will generate route reply message this message called RREP, it is used by the source to know the path before sending the data packet from source to destination, AODV does not need to include total path for routing because the route process is created when RREP message moves hop by hop [4].

1.2 The Black Hole Attack

One of the most known and dangerous security threats which makes the performance of MANET weak is the Black hole (BH). It is a misbehavior node in the network which claims that it always has a path to destination to trick the network nodes [1].

When the source node sends RREQ to a node that is working as a black hole, it will send RREP to the source node to make it believes that BH has a fresher route to the true destination. Hence, the source node sends the data packets to BH instead of the true destination, in this case BH will delete these packets, and the data packets will not

Manuscript received August 5, 2016
Manuscript revised August 20, 2016

be delivered to the destination [2]. Black holes are divided into two categories the first category is Single Black hole attack, and the second category is Collaborative Black hole attack [10].

2. Related Work

Several solutions with different strategies have been presented to solve the black hole attack in MANET. For example:

Po-Chun Tsou, Jian-Ming Chang, Yi-Hsuan Lin, Han-Chieh Chao and Jiann-Liang Chen [5] proposed BDSR scheme for DSR based MANET. The BDSR strategy is based on using virtual address in order to force the malicious node to send RREP. BDSR strategy has been implemented based on DSR, the detection process depends on sending the RREQ from the source node, and BDSR can deal with single attack.

Deng, H., W. Li and D. Agrawal [6] proposed a solution for AODV based MANET, SIDSR source intrusion detection security routing mechanism depends on generating one more route to the intermediate node which sends RREP, this additional route is used for testing the existence of the route from the intermediate node to the destination node, the intermediate node can be considered as honest node If the route available, If not, the reply message from the intermediate node can be neglected, thereafter alarm message will be sent by the source node to the network nodes in order to make blocking for the malicious node.

SIDSR strategy is based on generating one more route. SIDSR strategy has been implemented based on DSR, the blocking process starts from the source node, and SIDSR can deal with single attack.

Maha Abdelhaq, Sami Serhan, Raed Alsaqour and Anton Satria [7] have proposed a solution. LIDSR local intrusion detection security routing mechanism strategy resembles the SIDSR strategy [6], however in LIDSR the previous node which locates near the malicious node it executes the detection. LIDSR strategy developed the detection process to be done locally and out of the source node, so LIDSR strategy adds some improvements to the SIDSR strategy.

LIDSR strategy is based on generating one more route. LIDSR strategy has been implemented based on DSR, the blocking process starts locally from the previous node of malicious node, and LIDSR can deal with single attack.

Mehdi Medadian and Khossro Fardad [8] proposed a solution for AODV based MANET this solution is called MAODV. The first node which receives a RREP packet will lead the judgment process of the replier. The judgment process involves the decision if the replier is malicious node or not depending on the opinion of neighbors nodes, the activities of the replier are monitored by the neighbors. The opinions of neighbors about the replier are gathered and sent. After that the result will be extracted as follow:

Rule one: the node will be considered as honest node If many data packets are submitted to the destination node by the node.

Rule two: If the node receives many packets, and does not send the same data packets then the neighbors will consider this node as a malicious node.

Rule three: if the node sends many RREP but it does not send the same data packets then the Judgment will be considering the node as a malicious node.

Rule4: the node is considered as a failed node , if the current node has not sent any RREP packets and if rule two is correct**.**

MAODV depends on the negotiation process with neighbors, and this solution detects collaborative/multiple black hole nodes in AODV based MANET.

Raj Shree, Sanjay Kr. Dwivedi and Ravi Prakash Pandey [11] proposed a solution for ZRP based MANET called Detection by broadcasting the bluff probe packet (S-ZRP). It uses a message with non existence address called bluff probe packet to detect the malicious node. By this strategy when source node broadcasts the bluff probe packet, it includes the address of virtual node. when BH reply, the source node detects and blocks it, and the source node asks the neighbors for updating their entries.

S-ZRP depends on sending bluff probe packet, and this solution can detect collaborative/multiple black hole nodes in ZRP based MANET. By this solution the detection process starts from the source node.

3. LIDBPP Overview

LIDBPP has been proposed in order to reveal and prevent the black hole attack in MANET with implementing AODV routing protocol. LIDBPP strategy depends on generating BLUFF message which includes a destination address which is not exist actually in the network, by this way LIDBPP will trick the malicious node. Moreover, LIDBPP has been proposed not only to treat the single black hole attack but also to treat the multiple and collaborative black hole attacks [9].

In LIDBPP the source node will generate the BLUFF message, the intermediate node will receive the BLUFF message, the true behavior is to broadcast this message to the neighbors because BLUFF message has a virtual address, but if the next node replies with RREP, it can be considered that the next node misbehaves and works as a black hole node. After blocking the black hole node the control will still with the previous node in order to send the BLUFF message to the node that locates after the black hole node, et cetera.

The control of detection and blocking will still with the previous node until the process reaches the last node, it is

obvious that the detection and cleaning process is serially executed this means that the control of process will not return to the source node [9].
LIDBPP depends on generating bluff probe packet, and this solution can detect collaborative/multiple black hole nodes in AODV based MANET. By this solution the detection process starts from the previous node so the detection process performed locally.
LIDBPP aims to perform the detection and blocking process effectively, and at the same time it aims to reduce the required message in order to minimize the network overhead, and LIDBPP avoids returning to the source node so as to reduce the time delay.

3.1 LIDBPP Algorithm

The Algorithm of LIDBPP is as in figure 1 [3] :

4. Simulation

There are many network simulators which can be used such as NS-2, and OMNET++, OPNET, and etc. In this paper NS-2 ver 2.33 is used because of many reasons: it is an open source, it is an object oriented, it can be used widely in various types of wired and wireless network, and etc.

4.1 Simulation parameters

The parameters of simulation are as in table 1:

4.2 The first simulation environment

In this part of simulation the number of nodes is changed in order to evaluate the performance of MANET according to the metrics average overhead, end to end delay and packet delivery ratio PDR, the comparison of this part includes LIDBPP and normal AODV.

4.3 Experimental Results

From Figure. 2 PDR of pure MANET and PDR of MANET with black holes are very nearby when implementing LIDBPP, but there is considerable difference between PDR of pure MANET and PDR of MANET under attack when LIDBPP is not implemented.
From Figure. 3 end to end delay of pure MANET and end to end delay of MANET with black holes are approximately equal when implementing LIDBPP, it is easy to notice that end to end delay is growing when number of nodes grow.
We can notice from Figure.4 that the number of nodes is directly proportional to network overhead, the curve of the average overhead of pure AODV based MANET is moving near the curve of the average overhead of LDBPP under attack, this means that the average overhead is approximately equaled in the two cases.

4.4 The second simulation environment

In the second part of simulation the number of black hole nodes is changed in order to evaluate the performance of MANET according to the metrics average overhead, end to end delay and packet delivery ratio PDR, the comparison of this part includes LIDBPP solution and MAODV solution.

4.5 Experimental results

In Figure.5 PDR of MANET with LIDBPP and PDR of MANET with MAODV are nearby, but there is a preference for LIDBPP.
In Figure. 6 the number of black hole nodes is directly proportional to network overhead, the curve of the average overhead of MANET with LIDBPP is slightly moving down the curve of the average overhead of MAODV based MANET, this means that the network overhead with LIDBPP solution is better than MAODV based MANET.
From figure.7 its clear that the curve of end to end delay of MAODV lies up the curve of end to end delay of LIDBPP. So that end to end delay of MANET with MAODV is greater when it is compared with MANET with LIDBPP.

5. Conclusion and Future Work

In this paper LIDBPP was used in MANET which is under attack and it was compared by simulation with AODV based MANET without any black hole attacks. It can be concluded from the simulation results of part one that the network performance of pure MANET and the network performance of MANET with LIDBPP solution are approximately identical with some differences, while the performance was measured with respect to network overhead, time delay and PDR, and It can also be concluded from the simulation results of part two that the network performance of MANET with LIDBPP solution is better than the network performance of MAODV based MANET while the performance was measured with respect to network overhead, time delay and PDR.
The simulation results in part one and in part two prove that LIDBPP solution has successfully stopped the black hole attacks and concurrently it has tried to pay attention to the performance.
So the process of developing this method has enabled us to detect and block the black hole nodes with high efficiency and less negative impact on MANET performance.
The research in the security of MANET is continued to find an optimal approach which may be developed by a

new scheme, it is expected from this scheme to keep the performance of MANET during the process of preventing the attacks.

References

[1] HizbullahKhattak, Nizamuddin, FahadKhurshid, "Preventing black and grey hole attacks in AODV using optimal path routing and hash", 987-1-4673-5200-0/13, IEEE, 2013.

[2] Fidel Thachil, K C Shet, "A trust based approach for AODV protocol to mitigate black hole attack in MANET", International conference of computer science, 978-0-7695-4817-3/12, IEEE, 2012.

[3] Imad I. Saada, Majdi Z. Rashad, Sherihan Abuelenin , " Various Solutions of Black Hole Attackin A mobile Ad Hoc Network (MANET) " , (IJCSIS) International Journal of Computer Science and Information Security, Vol. 12, No. 8, August 2014.

[4] Satoshi K., Hidehisa N., Nei K., Abbas J., and Yoshiaki N., "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, 2007.

[5] Po-Chun TSOU, Jian-Ming CHANG, Yi-Hsuan LIN, Han-Chieh CHAO, Jiann-Liang CHEN, (2011) "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", ICACT, 2011.

[6] Deng, H., W. Li and D. Agrawal,. "Routing security in wireless ad hoc networks". IEEE communications magazine, 40(10): 70-75, 2002.

[7] Maha Abdelhaq, Sami Serhan, Raed Alsaqour, Anton Satria, "Security Routing Mechanism for Black Hole Attack over AODV MANET Routing Protocol", Australian Journal of Basic and Applied Sciences, 2011.

[8] Mehdi Medadian, Khossro Fardad, "Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol", European Journal of Scientific Research, 2012.

[9] Imad I. Saada, Majdi Z. Rashad, "Local Intrusion Detection by Bluff Probe Packet (LIDBPP) in a mobile Ad Hoc Network (MANET)", IJCSIS International Journal of Computer.

[10] Science and Information Security, issue Vol. 11 No. 8, August 2013.

[11] Heta Changela, Amit Lathigara "A Survey on Different Existing Technique for Detection of Black Hole Attack in MANETs", International Journal of Science and Research (IJSR), Volume 4 Issue 1, January 2015.

[12] Raj Shree, Sanjay Kr. Dwivedi, Ravi Prakash Pandey, "Design Enhancements in ZRP for Detecting Multiple Black Hole Nodes in Mobile Ad Hoc Networks", International Journal of Computer, 2011.

Let N0: source node, and let the intermediate nodes are N1,N2.....Nn...N.n+1, let RREQr: RREQ with real address for the destination, and RREQb: BLUFF message with virtual destination address.

Step one: Source node N0
creates RREQ & do broadcasting for neighbors

step two: If (RREP is in the range of Hop Count Limit & Time Limit) Then
The nodes (neighbors) N1,N2.....Nn.Nn+1 examine the destination address
Else //RREP surpasses Hop Count & Limit Time Limit // Then
MANET network is pure MANET network
End If
If the destination address is real address Then
RREQ is considered as RREQr
Else RREQ is considered as RREQb
End if

Step three: If RREQr Then
The algorithm of normal AODV is selected

Step four: Else if RREQb & Nn send RREP to Nn-1 Then
The algorithm of LIDBPP is selected
A block control message will be created by Nn-1 and it will be sent to Nn
Nn will be blocked

Step five: Nn-1 will update its routing table
Nn-1 will send the updates to the neighbors
// All routes to the black hole node will be deleted from the routing tables of neighbors //
Else
Nn delivers RREQb to Nn+1
End if
End if

Figure 1: The Algorithm of LIDBPP

Table 1: Simulation Parameters

Parameter	Value
Simulation time	1200 s
Routing protocol	AODV
Transmission range	250 m
Traffic model	CBR
Pause time	2 s
Terrain area	1000 m * 1000 m
Total Number of nodes	70
Number of malicious node	1-3

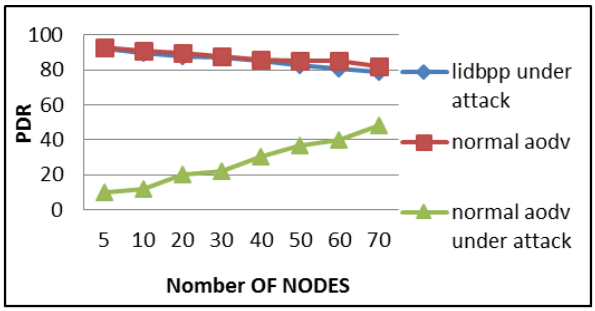

Figure 2 : number of nodes vs. PDR

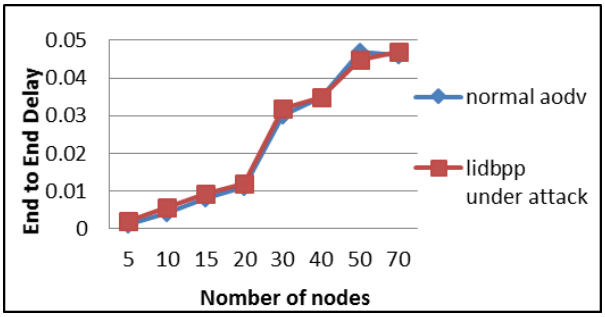

Figure 3 : number of nodes vs. end to end delay

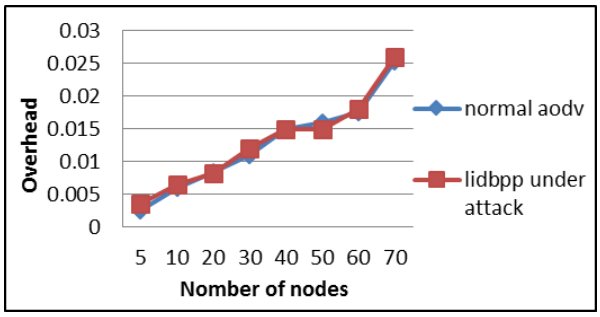

Figure 4 : number of nodes vs. overhead

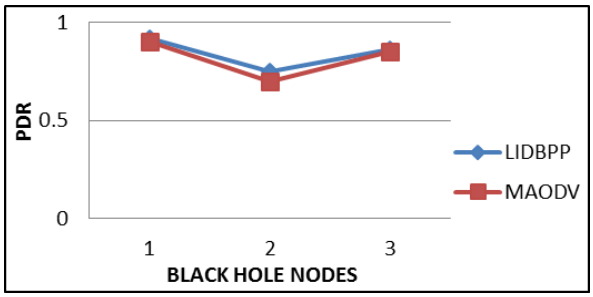

Figure 5 : black hole nodes vs. PDR

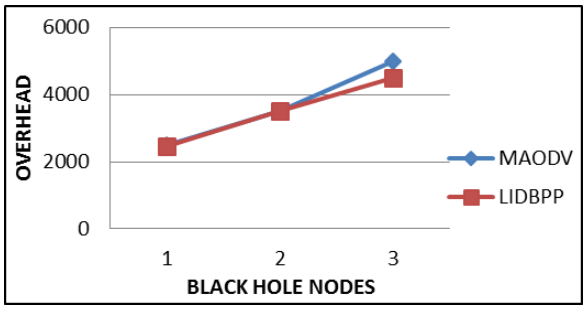

Figure 6 : black hole nodes vs. overhead

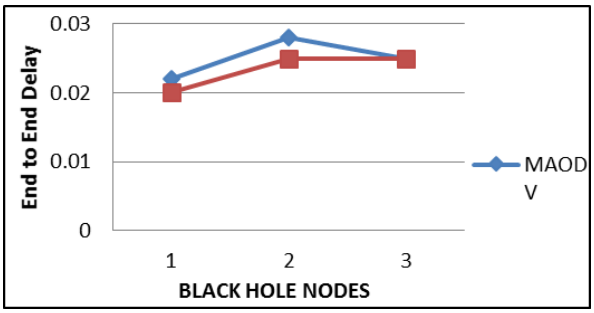

Figure 7 : black hole nodes vs. end to end delay