International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 4, August 2014, PP 75-78
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Security in Wireless Network: Black Hole Attack Avoidance

Ankit Sharma
Information Technology Engg., PIIT
New panvel, Navi Mumbai, India
asharma06@student.mes.ac.in

Manjusha Deshmukh
Computer Engg., PIIT, New Panvel
Navi Mumbai, India
manjudeshmukh@rediffmail.com

Abstract: *Wireless networks are computer networks that are not connected by cables of any kind. The use of wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. Wireless networks are susceptible to many attacks. One such specific attack is a blackhole attack in which malicious node falsely claiming itself as having the fresh and shortest path to the destination. In this paper, we propose a method for avoiding blackhole attack without the constraint of special hardware and dependency on physical medium of wireless network. The proposed methods forms link disjoint multi-path during path discovery to provide greater path selection in order to avoid malicious nodes in the path using legitimacy table maintained by each node in the network. By making use of bell curve, Non-malicious nodes gradually isolate the blackhole nodes and avoid them while making path between source and destination.Various related works were also studied for knowing the related works which have been carried out in order to avoid blackhole attack in a network. They had some flaws too,which were overcome by the proposed system.Proposed system helps us in defending against the blackhole attack without any requirement of hardware and special detection node.*

Keywords: *Blackhole, Wireless networks*

1. Introduction

One of the disadvantages of wireless network is security. To combat this consideration wireless networks may choose to utilize some of the various encryption technologies available, but some of them have weaknesses. Most of the previous research has focused on problems of routing for communication assuming a trusted environment. However, many applications run in untrusted environments and require secure routing for communication such as military or police networks, emergency response operations etc. A particular severe attack among several routing attacks is called blackhole attack [1]. In this attack, a malicious node tries to capture the path toward itself by falsely claiming larger sequence number and smaller hop count to the destination and then absorb all data packet without forwarding them to destination node. A blackhole can be formed either by a single node or by several nodes in collusion [2]. Blackhole attacks have serious impact on routing algorithms which uses sequence numbers to determine fresh messages and select the shortest route based on the hop count such as Dynamic Source Routing (DSR) or Ad-hoc On-Demand Distance Vector Routing (AODV).

2. Literature Survey

Shurman et. al.[1] proposed two different approaches to solve the blackhole attack problem. First, the sender node verify the authenticity of the node that initiates the RREP packet by utilizing the redundancy of the network. Second, each node store the last sent and received packet sequence number. If there is any mismatch then an alarm indicates the existence of a blackhole attack. However, this approach is unable to detect a multiple blackhole attack.

Tamilselvan el. al. [2] proposed an enhancement of the AODV protocol by introducing fidelity table. The RREPs are collected in the response table and the fidelity level of each RREP is checked and one is selected having the highest level. After acknowledgement is received, the fidelity level of the node is updated proving it safe and reliable. However, updating the fidelity table of each node by broadcasting it to other nodes results in congestion and also the selection of wrong RREP from the response table cause another route request flooding.

Marti et. al. [3] described the misbehavior detection using the watchdog and the pathrater. The watchdog identifies misbehaving nodes by listening promiscuously to the next node transmission whereas the pathrater uses the knowledge from the watchdog to choose a path that is most likely to deliver packets. This technique is imperfect due to limited transmit power, collison and partial dropping.

Burchegger et. al. [4] described the confidant protocol where each node monitor the behavior of its next hop and this information is given to the reputation system which makes decisions based on ratings about providing or accepting route from it. However, the use of reputation system makes this protocol impractical to include in adhoc network.an increase in the use of internet, there various attack being launched every day. These attacks target the vulnerabilities of various computer resources, such as, the operating system, web browsers, toolbars, etc.

3. Problem Statement

Black hole is an attack in wireless network in which malicious node falsely claiming itself as having the fresh and shortest path to the destination attract traffic towards itself and then drops it.In this project, we implement a system for avoiding blackhole attack without the constraint of special hardware and dependency on physical medium of wireless network.The project is divided into three modules.

4. Methodology

4.1. Software Architecture of BAAP

NS2 simulator is used for simulation. In the NS2 simulator Node object is already available. We will add a new variable in to make certain nodes as Black Hole Node if the node is Black Hole,the packet will be dropped on this node.Each node will be given their Node ID and position. Now a network is created with configurable number of nodes.Certain nodes can be made as Black Hole Node.Each node would find route to reach to their respective destination by making use of BAAP Routing Agent. We will vary the node speed and measure the delay in finding the route.We will vary the node speed and measure the packet loss. hole is an attack in wireless network in which malicious node falsely claiming itself as having the fresh and shortest path to the destination attract traffic towards itself and then drops it.In this project, we implement a system for avoiding blackhole attack without the constraint of special hardware and dependency on physical medium of wireless network.The project is divided into three modules.

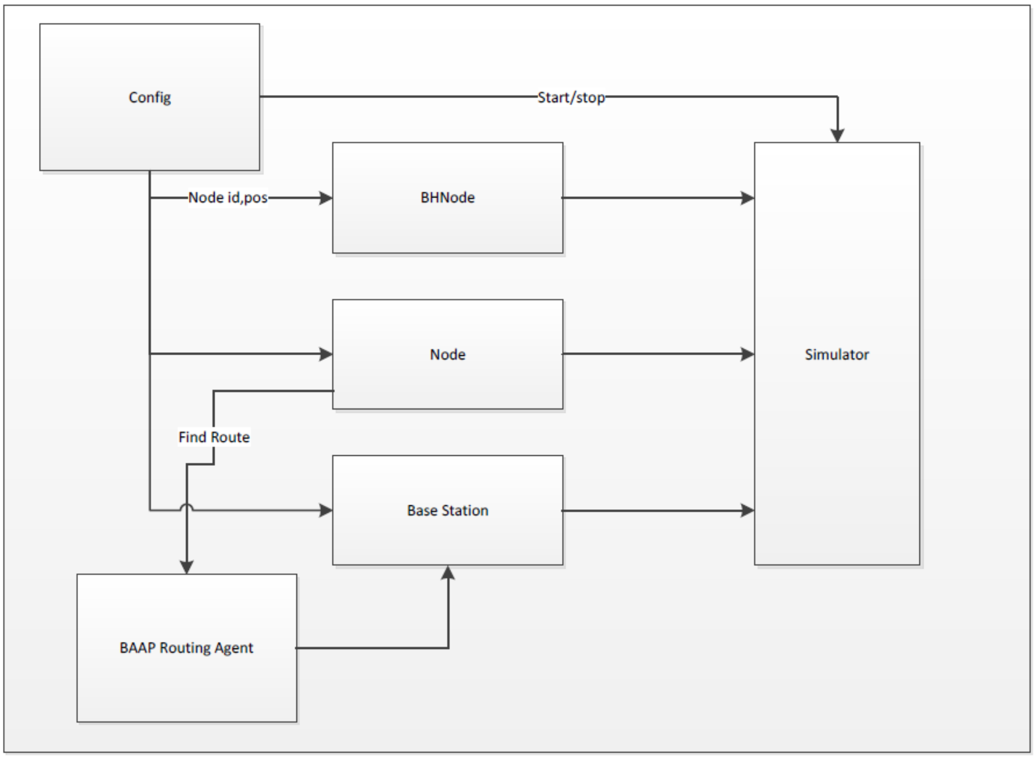

Fig1. *Methodology*

Level1. In level 1 the distance among the nodes are calculated using eucledian distance formula. This is one of the factor which is considered while selecting the route to reach the destination.

1. Let ‘i’ be n node present.
2. For i= 1 to n
3. i->broadcast the hello packet to all the neighbouring node
4. Estimation of distance between nodes calculated using eucledian distance √((X2-X1)^2+(Y2-Y1)^2)
5. Route discovery is done using routing table.

Pathcount basically specifies the number of times the nodes has been chosen in the route and the Sentcount field describes the number of times connection to destination have been successful node. This helps us in finding the legitimacy ratio of each node. A higher legitimacy ratio means higher possibility of a node being non-malicious [5].

6. Legitimacy ratio is calculated using sentcount and pathcount Sentcount/(Pathcount+1)

Level2.

7. If packet drop is greater than 95%, node will be considered blackhole node or malicious node.

The term bell curve is used to describe the mathematical concept called normal distribution. It refers to the shape that is created when a line is plotted using the data points for an item that meets the criteria of “normal distribution”. The center contains the greatest number of a value and therefore would be the highest point on the arc of the line. This point is referred to the mean, but in simple terms it is the highest number of occurrences of an element. The curve is concentrated in the center and decreases on the either side. A bell curve graph depends on two factors,the mean and the standard deviation. The mean identifies the position of the center and the standard deviation determines the height and width of the bell. The rules [6] of a normal distribution are:-

The total area under the curve is equal to 1 (100%)

About 68% of the area under the curve falls within 1 standard deviation.

About 95% of the area under the curve falls within 2 standard deviations.

About 99.7% of the area under the curve falls within 3 standard deviations

In level 2, we are proposing a method of able to separate those nodes which are dropping the 95% of the packets received that is which falls within 2 standard deviations.

5. Conclusion

We have discussed the related works which were used in order to avoid blackhole attacks and their limitations. The performance of the proposed system would be measured on the basis of their Performance Analysis, Throughput Analysis After detecting blackhole attack,packet drop on blackhole attack.

With the help of legitimacy table, we are able to differentiate between the malicious node and non-malicious node. The node with the higher legitimacy ratio will be chosen for the data transmission. Bell curve helps us in letting us know which nodes can be a blackhole or malicious node, by making use of standard deviations and medians we are able to categorize in which area the node falls in.

The proposed system is helpful in defending against the blackhole attack without any requirement of hardware and special detection node. It also does not require significant changes in the working of existing AODV protocol, however it uses an additional Legitimacy table for avoiding malicious node to grab the path between source and destination. It was explained with the help of the software architecture..

Acknowledgements

I remain immensely obliged to Prof. Manjusha Deshmukh, for providing me with the idea of this topic, and for her invaluable support in garnering resources for me by way of information and

guidance. I would like to say that it has indeed been a fulfilling experience working with Prof. Manjusha Deshmukh.

REFERENCES

[1] M.A. Shurman, S.M. Yoo, and S. Park, “Black hole attack in mobile adhoc networks,” 42nd ACM Southeast Regional Conf., pp. 11-14,2004.

[2] L. Tamilselvan, and V. Sankaranarayanan, “Prevention of cooperativeblack hole attack in manet”, Journal of Networks, Vol. 3 (5), pp.13-20,2008.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehaviour in mobile adhoc networks”, Proceedings of the ACM Conf. on Mobile Computing and Networking (Mobicom), pp. 255-265,2000.

[4]] S. Buchegger, and J. Le Boudec, “A testbed for misbehavior detection in mobile adhoc networks-how much can watchdogs really do”, Technical Report IC/2003/72 EPFL-DI-ICA. pp. 32-41, 2003.

[5] Saurabh Gupta, Subrat Kar and S Dharmraja, “BAAP:Blackhole Attack Avoidance Protocol for Wireless Network”, International Conference on Computer & Computer Technology/978-1-4577-1386-611/IEEE,2011

[6] David Kotz,Kobby Essien, "Analysis of a Campus Wide Wireless Network", Wireless Networks 11,115-133,Springer Science,2005.