http://dx.doi.org/10.21742/ijacis.2019.3.1.02

Analysis of Black Hole Attacks on Wireless Sensor Networks

K. Varaha Samba Murthy Raju[1], Y Bhargavi[2]

Dept. of Computer Science & Engineering, Vignan's Institute of Information Technology, Visakhapatnam, AP, India
murthy.111@gmail.com

Abstract

Wireless sensing element networks contains of assorted variety of freelance sensing element units and nodes that were accustomed to monitor and live the physical properties of assorted devices and conjointly the temperature and its connected measurements etc. The key applications of those units square measure the military, setting, unsafe places wherever it's troublesome for the masses to enter. A number of the necessary restrictions or the bounds of a sensing element network which is able to play a significant role on the performance of those kinds of networks. By considering these drawbacks, the sensing element networks is simply attacked by different devices or the different set of users within the same networks or other set of networks. This type of attacks within the wireless sensing element networks was thought of here and therefore the performance of the networks below these attacks was simulated by victimization the NS2 machine. When simulation, the result shows that the performance of the network may well be influenced by the presence of assorted set of attacks within the networks. Conjointly the importance was given to the amount of nodes being attacked during a single network.

Keywords: *Black hole attacks, Wireless sensor networks, NS 2 simulator*

1. Introduction

A Wireless device Networks are created and developed with numerous sorts and totally different sensors that may be used and applied to watch, observe and live the assorted physical and ecological conditions like temperature with vary of extreme temperature or the coldness, humidity, pressure etc. The design model of a wireless device network was ascertained within the following figures within the below section. The Wireless device Networks are developed by exploitation many numbers in a whole bunch and thousands of finding stations notable them as nodes at that every node within the network connected with different sensors [1][2].

The design of a Wireless device Networks consists of a radio transceiver that works as each as Associate in Nursing transmitter and receiver, Associate in Nursing antenna that may be used as each for internal and external applications for following the signals from numerous levels of signal and numerous strengths, a microcontroller unit for process the information that was being collected from numerous sensors and their connected units and additionally consists of A battery unit for provision the backup power for operating of many devices that were being developed and incorporated within the unit.

Article history:
Received (March 27, 2019), Review Result (June 3, 2019), Accepted (September 15, 2019)

Print ISSN: 2208-1658, eISSN: 2208-1666 IJACIS
Copyright ⓒ 2019 GV Press

A number of the most important applications of the device networks that may be deployed at numerous places and collects the information from all those networks and may be used for additional process of the information number of those applications are listed within the below figure and may be followed for clear image of the applications and their connected areas of the device networks [3].

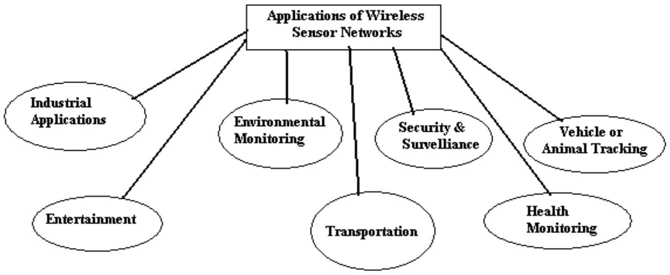


Figure 1. Applications of a wireless sensor network

2. Introduction to NS-2 simulator

Network machine a pair of was one among the principally used simulators for analyzing the performance of the network within the space of communication networks. The most important advantage of exploitation of the NS a pair of machine was to investigate and determine the varied attacks within the wireless detector networks [4][5]. These attacks are known and might be analyzed clearly by the usage of those sensors within the elaborated manner. The machine was the time based mostly machine and therefore the operating of the machine was determined within the kind of an incident driven machine.

The security within the networks is known simply and might be understood simply by the observation of varied attacks like denial of service which incorporates how-do-you-do flood attack, sink attacks, region attack etc. These attacks is known, tested and analyzed within the network such to make sure the information transmission between the nodes within the network during a secured fashion [6][7]. The following figure within the section below represents the essential design model of the NS2 machine. The name of the code that was developed or written was saved as an area of the execution associated it had been named because the TCL script of simulation and it had been passed as an argument to the input to machine for any type of application that was aiming to be enforced or tested by the utilization of this machine.

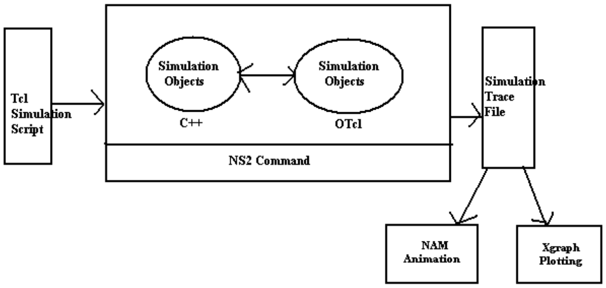


Figure 2. Basic architecture of a NS2 simulator

The files that were being generated from a simulator after executing or implementing a project or a task by a simulator was simulation trace file and the current file was utilized in a high fashion. The utilized file generated was mainly used for various applications like the generation of the graphs or plotting a graph and the other type of application was the animation related applications in the machines. The data that was being generated from the trace file was the NAM file for the animation applications purpose and the second usage of the trace file was to design and analyze the Xgraph for plotting or drawing a graph using the results from the simulation model.

3. Introduction to proposed system

Wireless device networks have terribly immense variety of applications that may be utilized in several areas of analysis and teachers. Providing security to the prevailing device networks or the networks that will be ready to style and work with the established network was of fine concern to be taken into the mind. Thus providing security to the info in networks was an honest concern in terms of the networks. The device networks area unit greatly prone to several attacks as a result of the presence of many constraints within the network [8]. A number of the attacks that we tend tore being thought of within the networks whenever we area unit operating with a device network in an exceedingly machine were the attacks and a few of the illustrious attacks that were determined within the device networks area unit the denial of service, sinkhole, and region and hi flood attack. By analyzing the machine, the small print concerning the attack, the characteristics of the attack and therefore the kind and nature of the attack were also studied thoroughly. With the results that were being generated from the simulated results, the behaviour of the network underneath varied masses and varied conditions was studied and therefore the performance of the network also can be examined thoroughly with valid results and proofs.

4. System design and architecture

The following figure displays and explains the fundamental model of the wireless detector network and additionally explains the mode of association created between the varied nodes were connected within the network. The most a part of a network was the ability generator that may well be wont to generate the ability that was needed by all the units within the network to figure properly and additionally to receive and transmit the information that was being generated and analyzed by the network supported the wants of the user. The information that was being collected by the detector was processed at the current unit within the format that was being needed by the network for additional processes.

The main goal or the intention of coming up with the processing unit within the network model was to method the information that was being collected from the sensors for additional higher cognitive process or to activate the bound set of conditions or management betting on the results that were being generated or sent from the sensors that were deployed at numerous locations within the field. The opposite units within the network model are the position finding system and also the mobilize unit for other connected works within the network unit placed or set at numerous locations within the field.

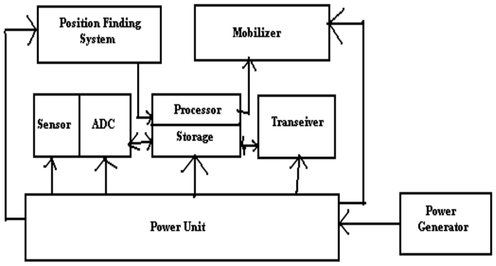


Figure 3. The components of a sensor node

5. System implementation

5.1. Configuring network simulator

In general, the wireless sensing element networks square measure substantially vulnerable to numerous attacks within the real-time surroundings eventualities. once the attacks square measure occurring at numerous points within the network, many issues could arise during which some issues square measure avoided and simply managed wherever as some issues square measure harder to resolve or avoid and in some cases the issues may result in the closing of the network or to cancel the network for its any process or operating conditions. The key attacks within the wireless sensing element networks square measure principally classified into 2 varieties supported the issues that were discovered within the networks until these days. The machine consists of broad range of applications, protocols like transmission control protocol, UDP and plenty of alternative network parameters for the development of the performance of the network.

5.2. Node creation and the connection between the nodes in the simulator

The coming up with of the network model within the machine was the initial task we've to begin whenever we want to form a project within the machine and to review the behaviour of the network in a very machine. The primary step within the coming up with or developing the network model within the machine was to form the amount of nodes within the network. the amount of nodes that the user planning to produce within the simulation model project was obsessed on the essential necessities of the user and also the user was given full freedom of making the amount of nodes to every project because the necessities of the project. The nodes within the model will be created dynamically in nature.

The user within the network will build any kind of modification to the nodes within the network as he desires by getting into the small print of the supply node, the destination node and also the malicious node which will be created or will be assumed by the user specified to research the behavior of the network or the performance of the network. The positions of the nodes and the movement of the nodes within the network at any purpose of your time will be generated and can also be analyzed and also the nodes can be partitioned off into many zones supported the need of the user and his project necessities for higher understanding and analysis of the network performance in a very higher and correct manner.

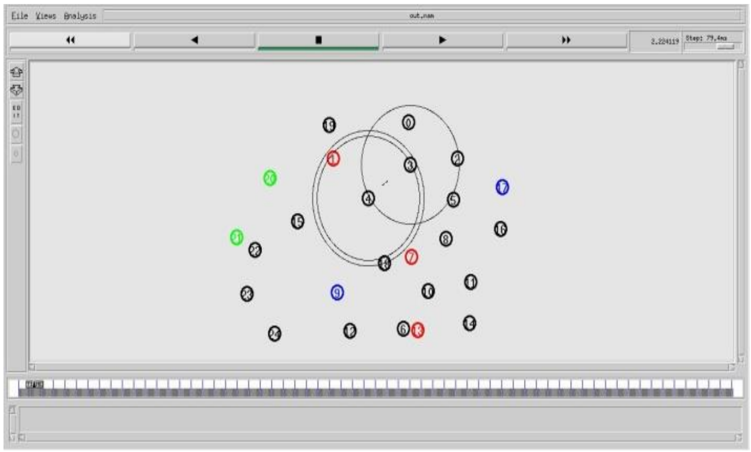


Figure 4. Creation of nodes in the simulator

When we got to begin the simulation method of the project, 1st of all the creation of the nodes should be done initially, a sure association that was renowned to the designer should be established between varied nodes within the network. The foremost necessary and known protocols that may be employed in varied sensing element networks or different set of wireless networks are the UDP and TCP protocols. These protocols are used largely for the operating of the networks in varied modes and conditions. TCP is that the association minded operating protocol that may facilitate in providing the packet received at the top user acknowledgement to the users. The necessary protocol used for sensing element networks and other set of networks was the UDP protocol. This protocol is generally employed in the cases wherever the large quantity of traffic was known and ascertained within the network system that was noticeably economical for the analysis of the performance of the network. This protocol consists of 2 components. The primary half was the TCP agent and also the second half was the TCP sink. There is a TCP agent and a TCP sink within the protocol half which might be utilized by the users for implementing each tasks just like the causing or the transmission of the info through the network and also the receiving of the info through the protocol.

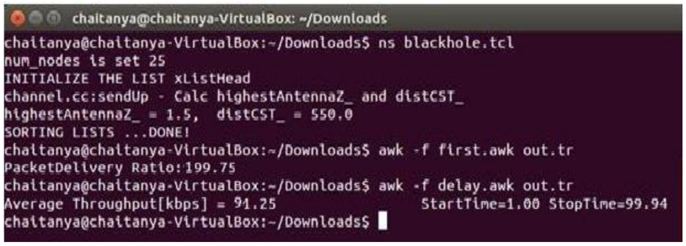
5.3. Simulation of black hole attack

Black Hole attack is taken into account jointly of the foremost vital kinds of attacks which will be ascertained within the wireless sensing element networks. it’s one amongst the foremost harmful and dangerous attacks that any sensing element network are often observe whenever we have a tendency to square measure addressing the attacks in sensing element networks [5]. During this sort of attack, an extra exterior contender is developed on a set of sensing element nodes within the wireless networks. The contender can build the nodes within the network such these nodes weren’t able to transmit any information to the opposite} nodes within the same network and different nodes within the other networks. Conjointly these nodes can build the changes within the program of the nodes such the info packets cannot be able to transmit even the nodes within the same network too. The simulation tool that was wont to carry this model of study was the NS2 machine. It’s able to complete by modifying aodv.cc come in ns2.35 which might be shown by plummeting the packets within the machine. [Figure 4] shows the simulation model of the region attack in a very wireless sensing element network.

The quantity of nodes that were being under fire within the network square measure studied as exaggerated from zero nodes attacked, two nodes attacked and 4 nodes being attacked by the mechanism and therefore the behaviour of the network was studied. The results were analyzed and mentioned within the following section with careful outputs and therefore the mean variety of packets delivered at the receiver finish. The outturn of the network and the mean variety of packets delivered are ascertained for the results and therefore the values within the numerical format square measure displayed within the tabular format within the following sections.

Case 1:

Packet delivery ratio and average throughput of a network without attack (5 black hole nodes) can be seen in the following figure. The first case was taken as the no nodes in the network model were not attacked. The simulation was performed and the various performance metrics were studied such that the results were displayed in the network model.

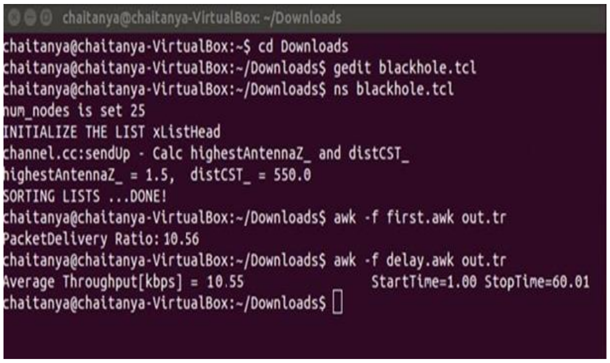


```
chaitanya@chaitanya-VirtualBox:~/Downloads$ ns blackhole.tcl
num_nodes is set 25
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
chaitanya@chaitanya-VirtualBox:~/Downloads$ awk -f first.awk out.tr
PacketDelivery Ratio:199.75
chaitanya@chaitanya-VirtualBox:~/Downloads$ awk -f delay.awk out.tr
Average Throughput[kbps] = 91.25            StartTime=1.00 StopTime=99.94
chaitanya@chaitanya-VirtualBox:~/Downloads$ █
```

Figure 5. The simulation model and the code for the first case of attacks in the network

Case 2:

Network with 15 black hole attack nodes: The second case of the work so far done in the present model was that the twenty nodes in the taken network model of wireless sensor network were being attacked. The two nodes attacked were considered as the change in colour in the figure shown and the performance of the network was analyzed with respect of various parameters. The attack had made some considerable impact on the performance of the wireless network so far considered and the results were represented in the form of tabular.

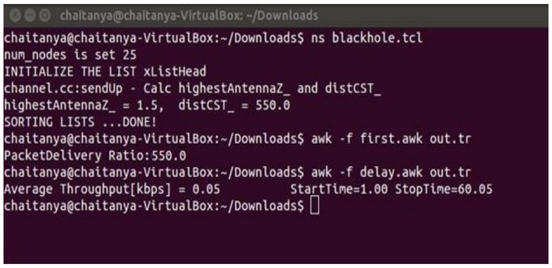


```
haitanya@chaitanya-VirtualBox:~$ cd Downloads
haitanya@chaitanya-VirtualBox:~/Downloads$ gedit blackhole.tcl
haitanya@chaitanya-VirtualBox:~/Downloads$ ns blackhole.tcl
um_nodes is set 25
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
ighestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
haitanya@chaitanya-VirtualBox:~/Downloads$ awk -f first.awk out.tr
PacketDelivery Ratio:10.56
haitanya@chaitanya-VirtualBox:~/Downloads$ awk -f delay.awk out.tr
Average Throughput[kbps] = 10.55            StartTime=1.00 StopTime=60.01
haitanya@chaitanya-VirtualBox:~/Downloads$ ▯
```

Figure 6. The simulation model and the second case of attacks in the network

Case 3:

Network with 40 black hole attack nodes: The second case of the work so far done in the present model was that the forty nodes in the taken network model of wireless sensor network were being attacked. The two nodes attacked were considered as the change in colour in the figure shown and the performance of the network was analyzed with respect of various parameters. The attack had made some considerable impact on the performance of the wireless network so far considered and the results were represented in the form of tabular.



```
chaitanya@chaitanya-VirtualBox:~/Downloads$ ns blackhole.tcl
num_nodes is set 25
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
chaitanya@chaitanya-VirtualBox:~/Downloads$ awk -f first.awk out.tr
PacketDelivery Ratio:550.0
chaitanya@chaitanya-VirtualBox:~/Downloads$ awk -f delay.awk out.tr
Average Throughput[kbps] = 0.05          StartTime=1.00 StopTime=60.05
chaitanya@chaitanya-VirtualBox:~/Downloads$ ▯
```

Figure 7. The simulation model and the third case of attacks in the network

5.4. Results

The performance of the wireless detector network system that we have a tendency to we have a tendency tore thought of was studied beneath varied conditions of the input that we were submitting to the system. The input of the system was being modified for 3 cases and also the performance was studied. The 3 cases were taken because the range of nodes of the network is being attacked in type of part attack. The primary case contains of the part attack that materialized on this network with no nodes were being attacked by the nodes within the network. The performance metrics just like the mean range of packets that were being delivered by the network at the receivers finish. The second case that we have a tendency to have thought of where the 2 nodes within the network being attacked beneath part attack and also the influence of the attack on the performance of the network was studied.

The third case we have a tendency to have thought of within the gift work was the four nodes of the whole nodes within the network were being attacked by the part attack. The performance was analyzed and also the results were being tabulated. By perceptive of these results, it's understood that the influence of part attack on the detector network might need smart impact on the performance of the network in term s of metric just like the quantity of packets being delivering at the receiver finish and also the turnout of the network the least bit the cases. The results that were being generated from all the 3 cases were tabulated and that they were given within the below tabular format.

Table 1. Results delivered from the simulation model for all the three cases

S.No	No.of Black Hole Nodes	Packet Delivery Ratio	Average Throughput
1	5	180.69	89.56
2	15	16.25	15.65
3	40	2.450	0.09

6. Conclusion

Wireless sensing element networks are getting used by most of the individuals within the society because of their significant helpful things to the common person within the society. The usage of those networks depends on the opposite necessary purpose just like the process capability to method the info and additionally to store the info for long amount of your time. They'll transmit the info very quickly to the most station because the memory was little for them to store. As a result of the on top of benefits and drawbacks, the providing security to the info was additionally massive task and downside. The performance metrics just like the packet delivery to the destination and also the output of the network were analyzed such to research the behaviour of the network beneath attacks. The results show that the attacks on the amount of nodes being attacked during a wireless sensing element network were having an honest impact on the performance of the network.

References

[1] Prabhakar. M. Kuldeep Sharma, and Neha Khandelwal, "An overview of security problems in MANET," Oriental journal of computer science and technology, vol.10, pp.82-85, **(2016)**

[2] Li, Wenjia, Joshi, and Anupam., "Security issues in mobile ad hoc networks -a survey," White House Papers Graduate Research in Informatics at Sussex, vol.17, pp.1-6, **(2008)**

[3] Arya Chandrakala and Arya Shobha, "Malicious nodes detection in mobile ad hoc networks," journal of Information and Operations Management, vol.3, no.1, pp. 210-212, **(2015)**

Copyright © 2019 GV Press

[4] Ghansela Siddharth, “Network security: Attacks, tools and techniques,” IJARCSSE, June, vol.3, no.6, pp.1-6, **(2013)**

[5] Chang R-S and Ting H-C, “Improving the performance of broadcasting in ad hoc wireless networks,” Journal of Internet Technology, vol.4, no.4, pp.209-216, **(2003)**

[6] Yang H, Lou H, Ye F, Lu S, and Zhang L, “Security in mobile ad hoc networks: Challenges and solutions,” IEEE Wireless Communications, vol.11, no.1, pp.38-47, **(2004)**

[7] Marti S, Giuli TJ, Lai K, and Baker M., “Mitigating routing misbehavior in mobile ad hoc networks,” Paper presented at the 6th annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, August, vol.10, no.4, pp.6-11, **(2000)**

[8] Yang S-J and Lin Y-C, “Static and dynamic RED tuning for TCP performance on the mobile ad hoc networks,” Journal of Internet Technology, vol.10, no.1, pp.13-21, **(2009)**