International Journal of Grid and Distributed Computing
Vol. 11, No. 12 (2018), pp.33-42
http://dx.doi.org/10.14257/ijgdc.2018.11.12.03

Black Hole Attacks on WSNs Using Discrete Simulator: An Extensive Review

N. Thirupathi Rao[1], Debnath Bhattacharyya [2], V. Madhusudhan Rao[3] and Tai-Hoon Kim[4*]

[1]Department of Computer Science and Engineering,
Vignan's Institute of Information Technology,
Visakhapatnam- 530049, AP, India
[2]Department of Computer Science & Multimedia,
Lincoln University College,
Kuala Lumpur, Malaysia
[3]Department of Chemical Engineering,
Vignan's Foundation for Science, Technology & Research
(Deemed to be University),
Vadlamudi, Guntur-522213, India
[4]Sungshin Women's University, Bomun-ro 34da-gil,
Seongbuk-gu, Seoul, Korea
[1]nakkathiru@gmail.com, [2]debnath@lincoln.edu.my, debnathb@gmail.com,
[3]budidampad1959@gmail.com, [4]taihoonn@daum.net

Abstract

Wireless sensor networks are becoming famous day to day due to the enormous applications and uses that these network models are providing. As the networks utilization was growing in a rapid manner day to day the attacks on these networks also gaining in a considerable manner. In the current paper, the effect of the presence of black holes in the network and their influence on the performance of the network was given thought and the implementation of such models are simulated by using NS2 simulator and the results are displayed in the results section.

Keywords: *Wireless sensor networks, black hole attacks, NS 2 Simulator*

1. Introduction to WSN

A Wireless Sensor Networks are made and developed with various types and different sensors that can be used and applied to monitor, observe and measure the various physical and ecological conditions like temperature with range of high temperature or the low temperature, humidity, pressure etc [1]. The architecture model of a wireless sensor network was observed in the following figures in the below section. The Wireless Sensor Networks are developed by using several numbers in hundreds and thousands of finding stations known them as nodes at which each node in the network connected with other sensors. The architecture of a Wireless Sensor Networks consists of a radio transceiver which works as both as an transmitter and receiver, an antenna that can be utilized as both for internal and external applications for tracking the signals from various levels of signal and various strengths, a microcontroller unit for processing the data that was being collected from various sensors and their related units and also consists of a battery unit for

Received (September 9, 2018), Review Result (November 8, 2018), Accepted (December 6, 2018)
* Corresponding Author

ISSN: 2005-4262 IJGDC

supplying the backup power for working of several devices that were being developed and incorporated in the unit [2].

Constructing, developing and establishing a wireless sensor network (WSN) has turn out to bea must and most required for collecting the data and processing the data at various places where the entrance to the normal humans has become very difficult. Various tasks and the works related to various tasks like the processing of the data in various formats and the collection and sensing of data from various places by using the several types of sensors with different applications and the communication of the presently working device with various other devices with their needs and other requirements that were being solved by using t6hese sort of networks [3]. The most common requirement and the issue to be followed while developing a wireless sensor network was to make the working of the system much easy and to monitor the working condition of the several sensors and the devices that were placed at various places at different locations where the humans will find very difficult to enter to such places. It is also very important point to be considered was that the providing security to various sensors that were placed at various different places such that to work independently to collect data from various sources and to transfer them to the required networks or the other set of sensor nodes. Several technologies were available in the market for the development of providing a good and excellent security for the working of the networks with which those networks were deployed to perform the operations [4].

In order to deploy the sensor nodes at various places and with a good number of sensors in number, the size of the sensor node should be always in a size of small for easy carrying and easy operations [5]. As the size of the device or the node decrease in size, the cost of the device also becomes very small and as the size of the device reduces, the working condition o0f the device increases and the operation of the devices becomes more easy and the size of the device also becomes very small. Some of those applications are listed in the below figure and can be followed for clear picture of the applications and their related areas of the sensor networks.

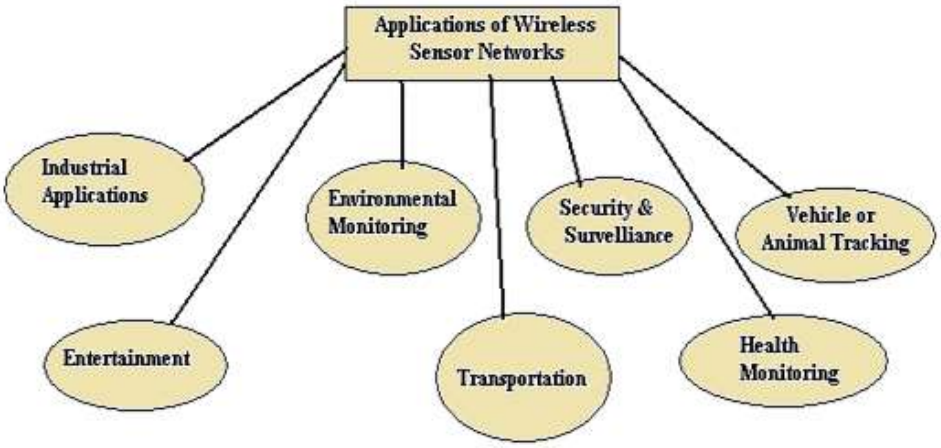

Figure 1. Applications of a Wireless Sensor Network

1.2. Introduction to NS2 Simulator

Network Simulator 2 was one of the mostly used simulators for analyzing the performance of the network in the area of communication networks. The major advantage of using the NS 2 simulator was to analyze and identify the various attacks in the wireless sensor networks. These attacks can be identified and can be analyzed clearly by the usage of these sensors in the detailed manner. The basic working of a simulator was very easy to operate and the implementation and observation of the simulator was very easy and it is

very near to the environment that can be observed in real time nature or environment. The simulator was the time based simulator and the working of the simulator was observed in the form of an event driven simulator.

Hence, the present simulator was termed or the simulator was taken as the event driven or the event dependent simulator. The programming code or the lines of code that can be written in such a way that the time on which particular time the event was happened and the time can be noted for the particular event that could happen at a particular point of time. The graphical user interface of the simulator was very easy to understand, operate and easy to cope up with the latest trends in the technology. It is very easy to understand the analysis of the transfer of data between the nodes and the set of attacks that were taking place in the sensor networks were also being monitored and understood easily by the use of the graphical user interface of the simulator [6]. As the features of the simulator are very easy and very easy to understand for the analysis and advantage of understanding the performance of the network and the behavior of the sensor network in terms of various parameters of the network. As a reason of this, the present simulator has become the most widely used simulator tool in the market for several applications and also the other advantage of the present simulator that it was an open source simulator. The present simulator is the free simulator which can be utilized for the various applications and it was utilized by several users mostly as it was a free open source simulator available in the market. The simulator can be downloaded free from the internet. The simulator and the associated files of the simulator were available in the online and can be downloaded by any valid user from the internet for their academic and research applications and their related areas.

The security in the networks can be identified easily and can be understood easily by the observation of various attacks like denial of service which includes hello flood attack, sinkhole attacks, Black Hole attack etc. These attacks can be identified, tested and analyzed in the network such that to ensure the data transmission between the nodes in the network in a secured fashion [7]. The following figure in the section below represents the basic architecture model of the NS2 Simulator. The present simulator network simulator model 2 was having a code of ‘ns’ which could be useful in utilizing the execution of the code which was written in the network simulator model 2. The name of the code which was developed or written was saved as a part of the execution and it was named as the tcl script of simulation and it was passed as an argument to the input to simulator for any sort of application that was going to be implemented or tested by the use of the present simulator. Once the execution of the project or the file or the task was being completed once, a trace of the simulation was created in the simulator which will help the users of the simulator to create or use some animation sort of applications or some applications which can be used for plotting a different types of graphical representations which includes the graphs [8].

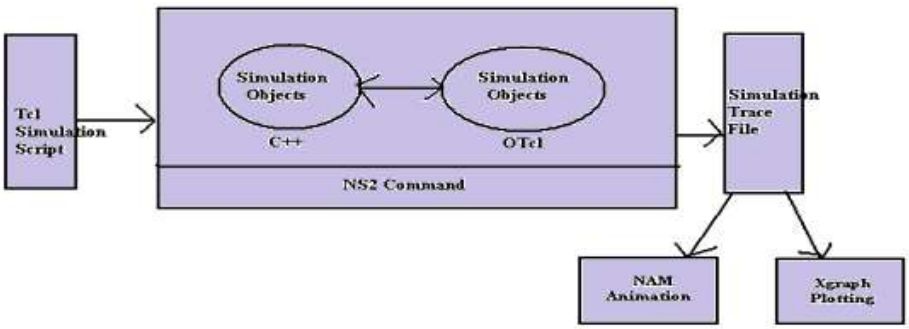

Figure 2. Basic Architecture of a NS2 Simulator

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.

1.3. Introduction to Proposed System

Wireless sensor networks have very huge number of applications that can be used in many areas of research and academics. The network can be useful deploying various places like where it becomes very difficult for human being to go such places and wait for a point of time and collect the data from those places and send that data to the base stations for further processing of the data. Providing security to the existing sensor networks or the networks that would be able to design and work with the established network was of good concern to be taken in to the mind. Hence providing security to the data in networks was a good concern in terms of the networks. The sensor networks are very much vulnerable to many attacks due to the presence of several constraints in the network. Some of the attacks that were being considered in the networks whenever we are working with a sensor network in a simulator were the attacks and some of the famous attacks that were observed in the sensor networks are the denial of service, sinkhole, and Black Hole and hello flood attack.

The presence of the above attacks or the occurrence of these types of attacks in a sensor networks will have a great impact on the network. The performance of the network might decreases and also the efficiency of the network also decreases with a noted type of values. The attacks that were observed in the network are studied in detail and were tried to analyze them and tried to solve such problems by the use of the simulator. By analyzing the simulator, the details regarding the attack, the characteristics of the attack and the type and nature of the attack were also studied in detail. With the results that were being generated from the simulated results, the behavior of the network under various loads and various conditions was studied and the performance of the network can also be examined in detail with valid results and proofs.

2. System Design and Architecture

The following figure displays and explains the basic model of the wireless sensor network and also explains the mode of connection made between the various nodes were connected in the network. The main part of a network was the power generator, which could be used to generate the power that was required by all the units in the network to work properly and also to receive and transmit the data that was being generated and analyzed by the network based on the requirements of the user. The generator provisions the power to the power unit. This supplies the power to the remaining units in the network such that to work for the task that was being allocated by the unit. The power was given to the sensing unit in which the sensor works and the data collection was being made by the sensor. The data that was being collected by the sensor was processed at the present unit in the format that was being required by the network for further processing.

The other important unit in the architecture model was the sensing unit. The sensing unit was a combination of both devices such as the sensor and the ADC units. The sensor used in this was unit was of different models as the sensor type was selected based on the requirements of the application it is going to be used or deployed in the field. The second part of the unit was the ADC unit which was the analog to digital conversion. The major task of the unit was to convert the data from analog model to the digital mode that can be

used in the computers or systems such that for further processing.The data that could be processed in all the machines was almost in the format of binary which was to be taken as the digital data and this data has to be converted by this ADC unit. The other important unit on the network model was the processing unit.

The main goal or the intention of designing the processing unit in the network model was to process the data that was being collected from the sensors for further decision making or to activate the certain set of conditions or control depending on the results that were being generated or sent from the sensors that were deployed at various locations in the field. The unit consists of the processor and the storage. The processor is responsible for processing the data that was being collected and also to process the units which were placed in the central unit such that for further processing the data. It also requires running the certain units present in the network unit. The other most important unit in the kit was the transceiver. It is a combination of both the transmitter and receiver for both transmitting the data from the network or from the sensor network and the receiver for receiving the data from other units which were placed at various different locations in the field. The other units in the network model are the position finding system and the mobilize unit for other related works in the network unit placed or located at various locations in the field.

3. System Implementation

3.1. Configuring Network Simulator

In general, the wireless sensor networks are very much susceptible to various attacks in the real time environment scenarios. When the attacks are occurring at various points in the network, several problems may arise in which some problems are avoided and easily managed where as some problems are more difficult to solve or avoid and in some cases the problems might be lead to the closing of the network or to cancel the network for its further processing or working conditions. The major attacks in the wireless sensor networks are mainly classified into two types based on the problems that were observed in the networks till today. The basic types of attacks in the wireless networks are the physical attacks and the logical attacks. Physical attacks are those in which the incarcerating the nodes and interfering the nodes which leads to the loss of data in the nodes.

Hence, the task of finding or identifying the attacks in the sensor networks was a very important feature or phenomenon which can be implemented or performed to increase the efficiency of the network. The simulation of the network model was one of the important options for the task that can be performed to identify the attacks in the sensor networks. NS2 simulator was one of the famous simulator that were available in the market for the last few years such that to identify the attacks in the sensor networks. The SN2 simulator was an open source simulator that was available in the market for online and offline users. It is the best suited and good utilized simulator for the utilization of the protocols like TCP and UDP protocols in the sensor networks for different applications. The simulator works on the language called Tool Command language (OTcl). With the help of this language, it has become very easy for the users and developers for analyzing and implementing the several important protocols and topologies in the networks. The main idea is behind this language is that this is the very easy language that everybody can learn easily and also can be implemented very easily in the real time environment by various number of users. The language is very easy to use and implement and similarly the language is platform independent which includes that anybody can use the simulator with different types of operating systems in their machines or computers at any point of time. The creation of the nodes or the deployment of nodes can be done by creating the lines of

code or writing the lines of code and also for displaying the transfer of data from various nodes in the network are done by writing certain lines of code in the simulator.

3.2. Nodes Creation and the Connection between the Nodes in the Simulator

The designing of the network model in the simulator was the initial task we have to start whenever we need to create a project in the simulator and to study the behavior of the network in a simulator. The first step in the designing or developing the network model in the simulator was to create the number of nodes in the network. The number of nodes that the user going to create in the simulation model project was dependent on the basic requirements of the user and the user was given full freedom of creating the number of nodes to each project as the requirements of the project. The nodes in the model can be made dynamic in nature. The user will be given full freedom of making changes to the nodes in entire project as he wishes whenever he is using the simulator for the purpose of making changes to the existing nodes or the existing network in the real time scenarios.

The user in the network can make any sort of change to the nodes in the network as he wishes by entering the details of the source node, the destination node and the malicious node that can be created or can be assumed by the user such that to analyze the behavior of the network or the performance of the network. He also have a choice of running or executing the simulator at any point of time he needs and also make changes in the network project as the nodes in the network model are dynamic. The positions of the nodes and the movement of the nodes in the network at any point of time can be generated and also can be analyzed and also the nodes can be partitioned into several zones based on the requirement of the user and his project requirements for better understanding and analysis of the network performance in a better and accurate manner.

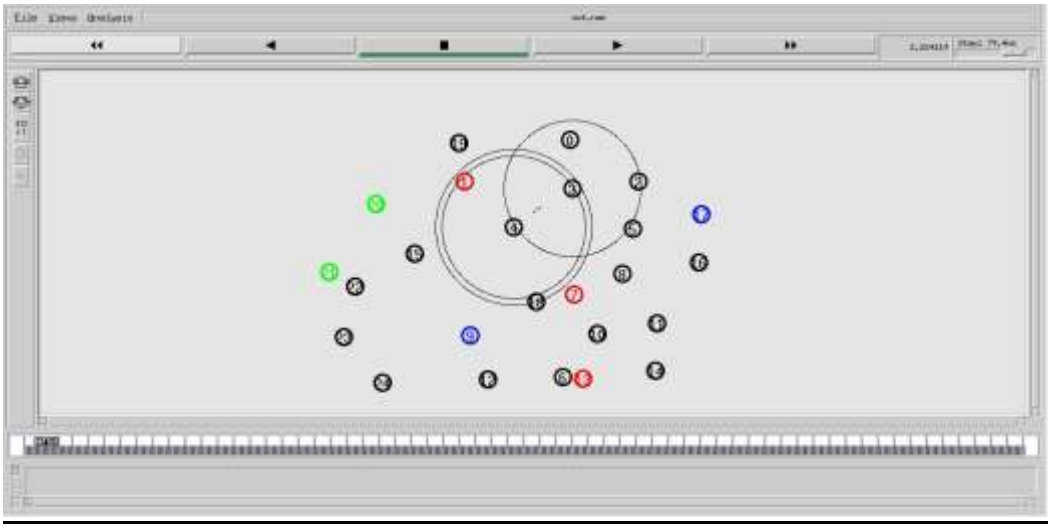

Figure 4. Creation of Nodes in the Simulator

When we need to start the simulation process of the project, first of all the creation of the nodes has to be done at first, a trusted connection that was known to the designer must be established between various nodes in the network. Several protocols that were available in the networks and especially in the sensor networks to implement the network models with the help of the protocols. The most important and famous protocols that can be used in various sensor networks or other set of wireless networks are the UDP and TCP protocols. These protocols can be used mostly for the working of the networks in various modes and conditions. TCP is the connection oriented working protocol that can help in providing the packet received at the end user acknowledgement to the users. The mostly used protocol in the networks and also in the internet applications which were

purely on the basis of networks with both the wired and wireless networks with various topologies those were available in the market. The other important protocol used for sensor networks and other set of networks was the UDP protocol. This protocol is mostly used in the cases where the huge amount of traffic was identified and observed in the network system which was very much efficient for the analysis of the performance of the network. This protocol consists of two parts. The first part was the TCP agent and the second part was the TCP sink.

There is a TCP agent and a TCP sink in the protocol part which can be used by the users for implementing the both tasks like the sending or the transmission of the data through the network and the receiving of the data through the protocol. TCP agent is accountable for transferring the packets in the network which can be known as a source node. The receiver node is the TCP sink which can be used to receive the packets which were sent from the receiver node.

3.3. Simulation of Black Hole Attack

Black Hole attack is considered as one of the most important types of attacks that can be observed in the wireless sensor networks. It is one of the most harmful and dangerous attacks that any sensor network can be observe whenever we are dealing with the attacks in sensor networks. In this type of attack, an additional exterior challenger will be developed on a subset of sensor nodes in the wireless networks. The challenger will make the nodes in the network such that these nodes were not able to transmit any data to the other nodes in the same network and other nodes in the other networks. Also these nodes will make the changes in the program of the nodes such that the data packets cannot be able to transmit even the nodes in the same network too. There are a lot of establishment that help in maintaining the individuality by means of documentation software's [5]. Black Hole attacks are the most common types of attacks. They are liable to confront the safekeeping and security of the system. There are a lot of customs to guard a structure from Black Hole attack. Trusted influence and good uniqueness can help avoid a network from such type of an attack.

The simulation study on the behavior of the wireless sensor network under this type of attacks on various numbers of nodes was studied. The simulation tool that was used to carry this model of study was the NS2 Simulator. It is able to complete by modifying aodv.cc file in ns2.35 which can be shown by plummeting the packets in the simulator. Figure 4 shows the simulation model of the of the Black Hole attack in a wireless sensor network. The attack was observed in various cases. Each case was considered with various numbers of nodes being attacked by the black hole problem. The analysis was done in such a way such that to study the behavior of the network under various conditions. The number of nodes that were being under attack in the network are studied as increased from zero nodes attacked, 2 nodes attacked and four nodes being attacked by the mechanism and the behavior of the network was studied. The results were analyzed and discussed in the following section with detailed outputs and the mean number of packets delivered at the receiver end. The throughput of the network and the mean number of packets delivered will be observed for the results and the values in the numerical format are displayed in the tabular format in 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.

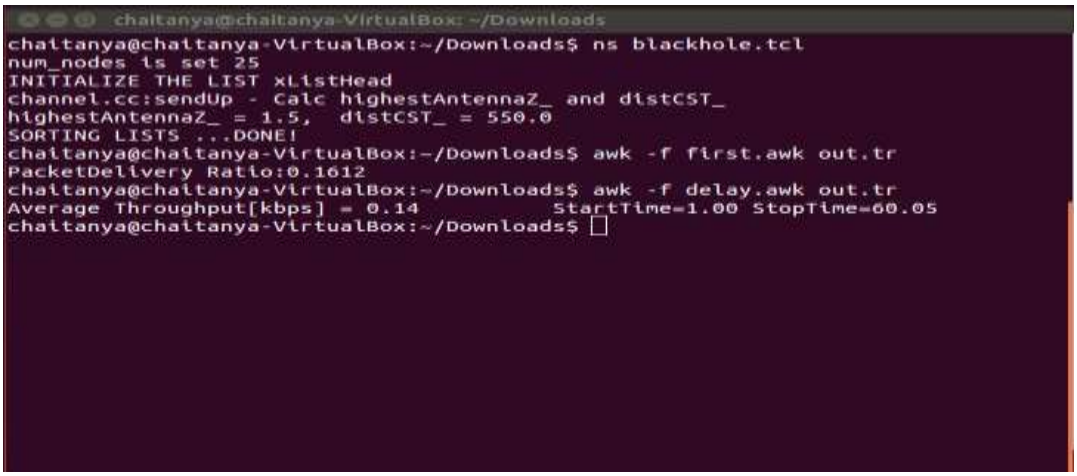

Figure 4. The Simulation Model and the Code for the First Case of Attacks in the Network

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 fifteen nodes in the taken network model of wireless sensor network were being attacked. The two nodes attacked were considered as the change in color 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.

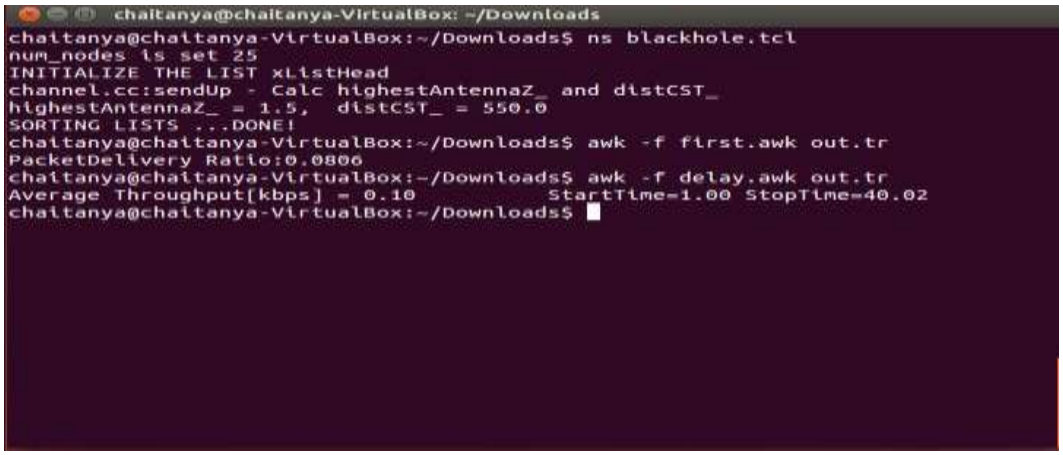

Figure 5. The Simulation Model and the Second Case of Attacks in the Network

Case 3:

Network with 25 black hole attack nodes:

The second case of the work so far done in the present model was that the 25 nodes in the taken network model of wireless sensor network were being attacked. The two nodes attacked were considered as the change in color 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.

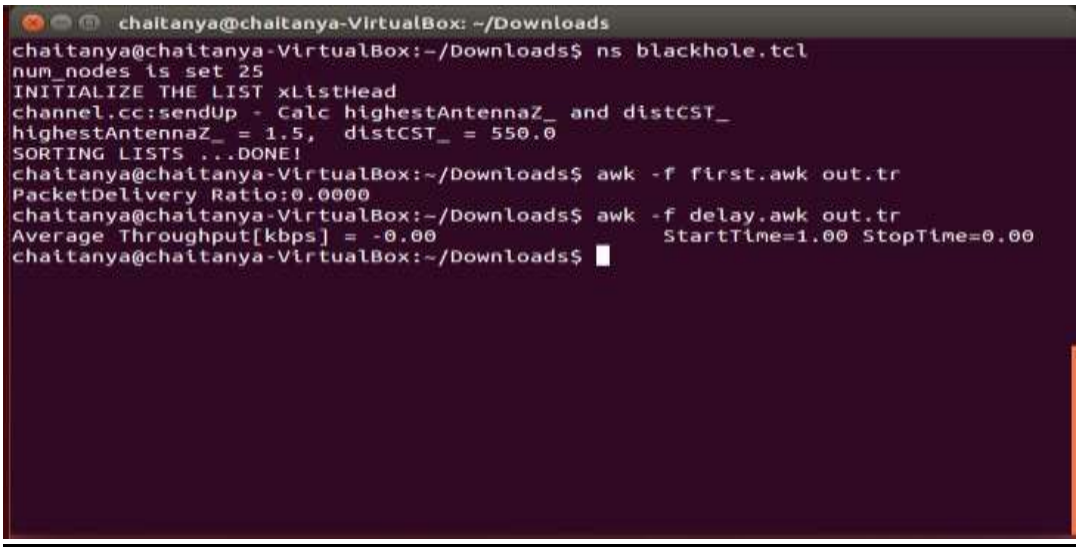

Figure 6. The Simulation Model and the Third Case of Attacks in the Network

4. Results

The performance of the wireless sensor network system that we were considered was studied under various conditions of the input that we were submitting to the system. The input of the system was being changed for three cases and the performance was studied. The three cases were taken as the number of nodes of the network being attacked in form of black hole attack. The first case comprises of the black hole attack that took place on the current network with no nodes were being attacked by the nodes in the network. The performance metrics like the mean number of packets that were being delivered by the network at the receivers end. The second case that we had considered were the two nodes in the network being attacked under black hole attack and the influence of the attack on the performance of the network was studied. The third case we had considered in the present work was the four nodes of the total nodes in the network were being attacked by the black hole attack. The performance was analyzed and the results were being tabulated. By observing all these results, it is understood that the influence of black hole attack on the sensor network might have good impact on the performance of the network in term s of metric like the amount of packets being delivering at the receiver end and the throughput of the network at all the cases. The results that were being generated from all the three cases were tabulated and they were presented in the below tabular format,

Table 1. Results Delivered from the Simulation Model for all the Above Cases

S.No	No.of black hole nodes	Packet deliveryratio	Average throughput
1	5	99.7583	51.25
2	15	20.2256	17.42
3	25	0.1612	0.14
4	40	0.0806	0.10
5	45	0.000	0.000

5. Conclusion

Wireless sensor networks are being used by most of the people in the society due to their heavy useful things to the common man in the society. They were very to carry and also to plant them at various places and also the size of the unit as very small and also the important thing to be considered was the consumption of the power that these units will consume when the users working with these sort of units in the society. Hence, as a result of all these advantages, the usages of this device are heavy in the market. The usage of these networks or these devices is also heavily suggested by the government authorities to use these days. As a result, the usage of these devices had growth a lot more on the market. Similarly, the disadvantage of these sorts of networks is the limited storage capacity of these units. The usage of these networks was depends on the other important point like the processing capacity to process the data and also to store the data for long period of time. They will transmit the data vary fast to the main station as the memory was very little for them to store. As a result of the above advantages and disadvantages, the providing security to the data was also big task and problem. As a result, the attacks on these devices were more and the data was being stolen and the more number of attacks were being under taken. The attacks that are popular in a WSN are the black hole attack has been simulated in a simulator. The simulation was studied for various cases of the node number in order to analyze the performance of the network at various levels of attacks on the nodes in the network. On simulation, the performance and the efficiency of the network can be analyzed. The behavior and the energy parameters can be examined. The performance metrics like the packet delivery to the destination and the throughput of the network were analyzed such that to analyze the behavior of the network under attacks. The results show that the attacks on the number of nodes being attacked in a wireless sensor network were having a good impact on the performance of the network.

References

[1] RichardKissel, Kevin Stine,and Matthew “Information Security” NIST Special publication 800-64 Revision 2, October2008.
[2] Wireless Communication, link http://www.atis.org/, Archived from theoriginal on 2008-01-02.
[3] Andrea Goldsmith, Wireless Communications, Cambridge UniversityPress, September 2005, ISBN13: 9780521837163.
[4] William Stallings, Wireless communications and networking, WilliamStallings books on computer and data communications Technology,Publisher Prentice Hall, 2002, ISBN10 0130408646, ISBN139780130408648, Length 584 pages.
[5] Jody L. Schivley “Network Security and the NPS Internet Firewall“September 1994.
[6] BasuDev, Shivahare, CharuWahi, ShaliniShivhare, “Comparison of Proactive and Reactive Routing Protocols in Mobile Adhoc Network using Routing Protocol Property”, ISSN 2250-2459, vol. 2, Issue 3, March 2012.
[7] NeerajBhargava, RituBhargavaAnchalKumawat, Bharat Kumar, “Performance of TCP- Throughput on NS2 by Using Different Simulation Parameters”, ISSN (print): 2249-7277 ISSN (online):2277-7970), Vol. 2 No. 4 Issue-6 December-2012.
[8] Bruno, R.; Conti, M.; Gregori, E.; “Throughput Analysis of UDP and TCP Flows in IEEE 802.11b WLANs; A Simple Model and Its Validation”, Workshop on Techniques, Methodologies and Tools for Performance Evaluation of Complex Systems, 2005. (FIRB-Pref 2005), pp. 54 – 63, 19 Sept. 2005.
[9] William Stallings, Wireless communications and networking, William Stallings books on computer and data communications technology, Publisher Prentice Hall, 2002, ISBN10 0130408646, ISBN13 9780130408648, Length 584 pages.

