IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Black Hole Attack, its Detection and Mitigation under AODV Routing Protocol in WSN using Expert System

[1]Naveen, [2]Pankaj Kumar Yadav, [3]Vimal Kumar, [4]Mani Singh

Dept. of Computer Engineering
Army Institute of Technology, Pune, India

Abstract: Wireless Sensor Networks (WSN) are divided into power and computer type networks that can be easily set up in remote locations with the help of mobile devices or nodes. Nodes in these Networks monitor and monitor local physical and environmental conditions and transmit this information to each other or remotely using Wireless Sensor Networks integration and integration methods. These networks play a key role in many areas such as military and civilian recruitment, health care systems and climate monitoring where manual learning is tedious or inefficient. Due to the self-configuration of wireless nerve networks or nodes related to their unprotected environment due to remote locations, various types of security attacks can occur on these networks. Black hole attacks or grey hole attacks are primarily an effective form of attack that can reduce the outflow and efficiency of the corresponding network connection which can also have a negative impact on the network. In this paper, we will understand the attacks of black holes and will review various ways to find and distinguish non-network space.

***Index Terms* – SDN, OpenFlow, Mininet, Blackhole attack**

I. Introduction to WSN

Wireless Sensor Network (WSN) is basically a distributed network of nodes where independent sensors and nodes are connected together in various applications. WSNs contain a number of visual channels called sensors nodes, each of which is small, lightweight and portable in construction. WSNs are twice-guided in the flow of data and their topology varies according to its corresponding system used for that. They have many important features such as: node mobility, heterogeneity, very high distribution rate, ease of use, ability to deal with node failures or attacks i.e., subsistence and more. The main function of the WSN sensor node in the WSN sensor is to detect events, perform local data processing, and send raw or used data to another places. The sink serves as the primary channel that plays a key role in the wireless environment and acts as a distributed controller. The Base station at WSN is important for the following reasons: node sensors are prone to failure so it helps to collect data better and provide a backup in case the master node fails anywhere.

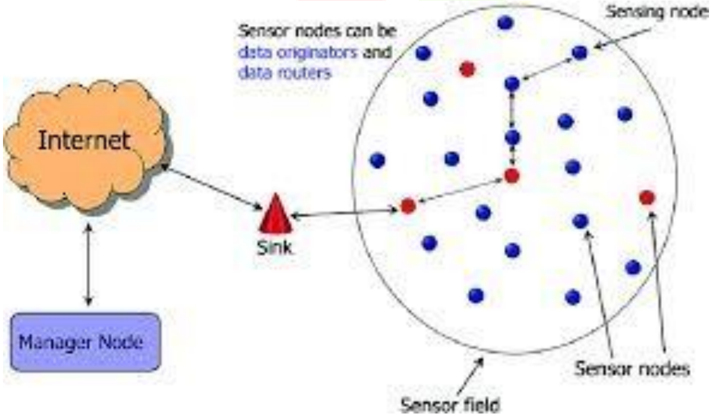

Figure 1. Design of a Standard Wireless Sensor Network

A. Features of WSN

1) Computer capabilities: Due to size limitations, the cost and power consumption of the battery as it is located remotely, system space and memory space for sensors and other nodes are very limited.
2) Battery power: Sensor signals are often inoperable and are discarded because the power is remotely located in its application.
3) Communication capacity: The communication range of Senor networks is very small and continuous. And the contact distance is only tens to several hundred meters. Even the sensors can be easily affected or controlled by rain and lightning, so it is difficult to maintain the proper functioning of these networks.
4) Dynamic Topology: Nodes can fail due to battery fatigue or various other reasons and new nodes can be added depending on the job requirements, leading to frequent network duplication.

5) Multi-hop communication: Sensor nodes can only communicate with neighbors directly in WSN. If one node needs to communicate with another in excess of the frequency of the node radio frequency it should be through multi-hop transmission through internal channels.

B. Challenges in WSN

Wireless nerve networks have great potential and growth because they will increase our ability to monitor and communicate away from the physical world in seconds. Sensors have the ability to collect large amounts of anonymous data for further processing. Sensors can be remotely accessed and placed where it is not possible to send data and power cables through humans. In order to harness the full potential of sensory networks, we must first address some of the limitations of these networks and their technological problems. Although data integration requires that nodes must be synchronized, the sync protocols used must address the characteristics of these networks. In order for these Networks to be ubiquitous, many challenges and obstacles must be overcome that do not result in the loss of privacy and confidentiality of shared information.

1) Energy: The first and most important challenge to making WSN is its energy saving. Power integration can be divided into three functional categories: Hearing, the Communication component, and the final component of each data processing process that needs to be done in its design and algorithm. The time node sensor used in a network system indicates a strong reliance on battery life. The most common obstacle associated with the construction of a sensor network is that the sensor nodes operate on a limited power budget.

Usually, the sensors are powered by batteries, which need to be replaced or reopened when they run out and it is quite a tedious task due to the remote locations. For non-rechargeable batteries, the sensor node must be operational until its mechanical expiration date or battery is replaced. The duration of the machines depends on the type of application to which we are sent.

2) Limited bandwidth: In wireless nerve networks less power is used in data processing than in transmission. Currently, wireless communication is limited to data rate at a rate of 10-100 Kbits / second.

The bandwidth limit directly affects the exchange of messages between the sensors used and synchronization is not possible without the exchange of messages. Sensitive networks often work on

restricted bandwidth and restricted functionality offline multi-hop wireless connectivity These wireless connectors operate in radio, infrared, or optical range.

3) Node Costs: The sensor network contains a large collection of node sensors. It means that the cost of each node is important for the total financial metric of the sensor network. Obviously, the cost of each sensor node must be kept low in order for global metrics to be acceptable. Depending on the use of the sensor network, a large number of nerve endings may be randomly distributed over the environment, such as weather monitoring. If the total cost was appropriate for sensory networks, then it would be very acceptable and effective for users who need careful consideration.

4) Transmission: Node transmission is an important issue that needs to be resolved in Wireless Sensor Networks. Proper node distribution scheme greatly reduces the severity of the problem. Installing and controlling the maximum number of nodes in a confined space requires special techniques. Hundreds of thousands of sensors can be sent to the sensory region. There are two current shipping models: (i) fixed shipping (ii) dynamic shipping. Vertical transmission selects a good location in terms of usage, and the location of the sensor nodes has no change in the life of the network. Powerful deployment throws nodes randomly for optimal use.

5) Security: One of the challenges for WSNs is to provide high security requirements for restricted resources. Remote activity and unsupervised sensory nodes increase their exposure to malicious intrusion and invasion. Security requirements on WSNs contain node authentication and data privacy. To identify both reliable and trustworthy nodes from secure positions, deployment sensors must perform node verification tests by their nodes that properly adjust cluster heads and unauthorized nodes can be separated from the network during the node authentication process.

II. SECURITY IS ATTACKED

Network security attacks are unauthorized acts or violations of private, corporate or government IT assets in order to destroy, alter or steal sensitive data from them. As many businesses invite employees to access data from mobile devices, networks are at greater risk of data theft or complete destruction of data or network. The following are the types of possible attacks on the network: -

- Passive Attacks
- Active Attacks

A. Passive Attacks

A casual attack on a computer, is an attack by an attacker that monitors communications or systems. Reading emails, trackinginternet usage and using a microphone or camera system to “spy” on a person or organization comes at this stage. In the unprovoked attack, the criminal

does not attempt to alter the system or alter the data but rather collects data that encrypts data privacy. The most common types of attacks are:

- Traffic Analysis
- Eavesdropping Pack
- Caution

B. Active Attacks

An effective attack, in computer security, is an attack by an attacker attempting to break into the system that hinders the integrity and availability of data. During an active attack, the hacker can enter data into the system and can change the data within the system. The types of active attacks are:

- Denial of Service Attack
- Worm infestation
- Sybil attacks
- Sinkhole Attack

III. ATWN BLACK HOLE ATTACKS

Blackhole attacks are a dangerous attack on the MANNET. In this attack, the negative environment captures the package from the source node itself by impersonating it as a destination learning destination. When a source node sends an RREQ message to all neighboring nodes during the route acquisition process, the malicious node immediately sends a fake RREP message to the source node before other nodes send RREP. Therefore, source nodes after receiving the first RREP from a malicious node reject all other RREPs from other neighboring nodes and thus monitor the completion of the Route Discovery process and send data packets to a non-node dark brown. By doing this all-data transfers between the source node and destination are disrupted and therefore system performance is compromised.

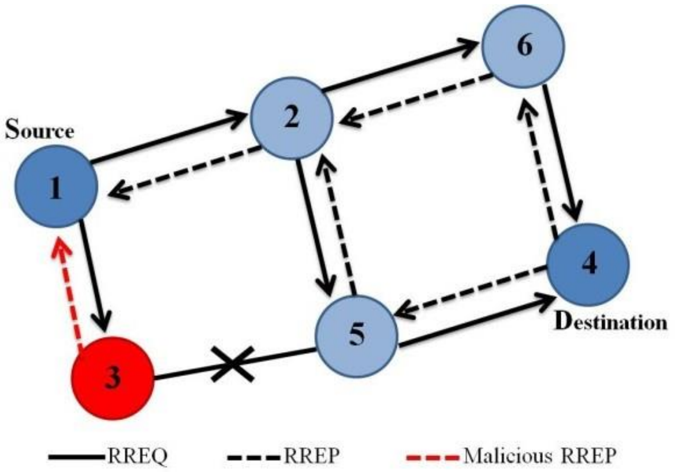

Fig. 2. Black Hole Node in WSN System

The effects of black hole attacks can be seen on WSN by the following comparison.

A. Package Delivery Rate

It is the average of the packets received by the destination in the total number of packets including discarded packets.

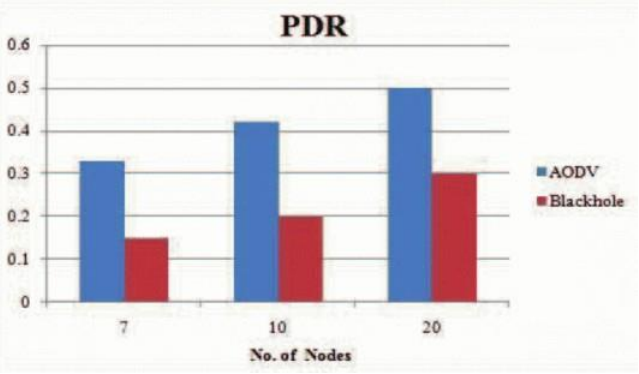

Fig 3. Packet delivery rate

B. Analysis of moderate delays

This can be defined as the number of delays that occur between packet delivery from the source node and receiving the package at its destination.

Includes all delays in all data flows such as packet duplication, billing and network access process.

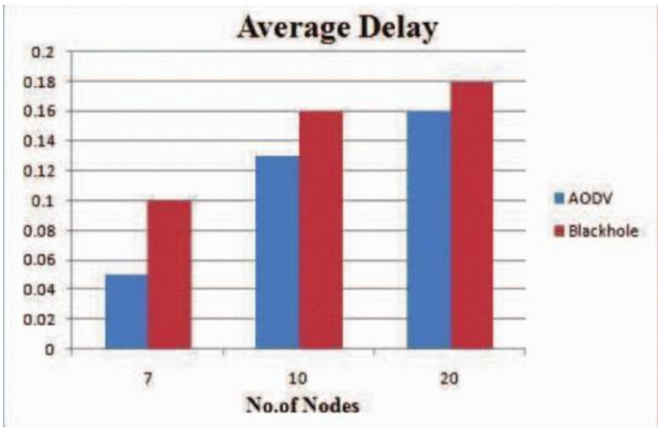

Fig. 4. Average Delay Analysis

C. Throughput

It is the amount of packet received by the destination cart for the total number of packets sent to the source node. Here, we see a significant impact of black hole attacks on wireless nerve networks.

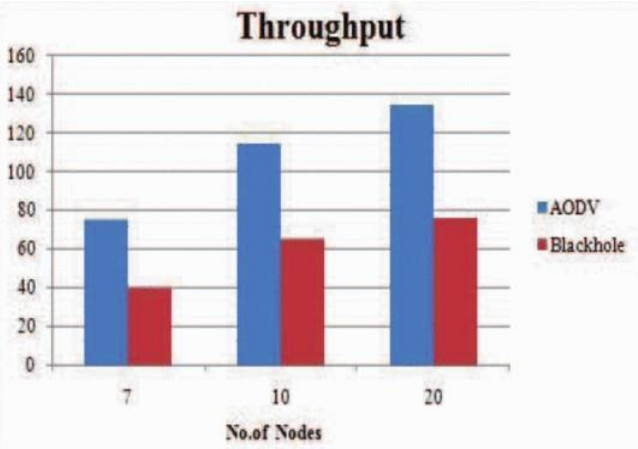

Fig. 5. Throughput

IV. EXPERT SYSTEM BASED INTRUSION DISCOVERY

Master Plan we have developed is called ADIOS: Advanced Discovery Sensor Networks that use a combination of viewing and a local expert system to make judgments based on the behavior of a neighbor's node when trying to identify network system attacks. This plan is based on the following assumptions:

The wireless network interface cards or NICs in the nodes used must be able to create a loose behavior mode that the node can feel and process the deployment of other nodes up and down again without being overstretched.

The antennas used on the nodes should be omni-directional as they support communication between different locations on WSNs.

There is a symmetry of dual connections between places

A. ADIOS System Development

The ADIOS Network program consists of five key elements: a lightweight professional program, expert information, a memory table, a multi-vote system and a watch dog program.

1) Weight Loss Expert System: The Weight Loss System (LES) is at the heart of our System and provides IDS-driven intelligence. Here machine thinking and distraction occur in the final decision-making process in relation to suspicious network work.
2) Expert Information: Expert information contains descriptions, rules and sequence of events that explain to LES what the black hole attack looks like. It can be modified to make this program work for other types of attacks such as Black Hole attacks.
3) Watchdog Program: This module contains a node interface card in loose behavior mode and has the ability to read and write to a table that resides in memory. It records the activity of interest in the table for LES to analyze on a causal basis.
4) Memory Storage Table: The MRT module is expected to be a system that supports most of the memory used by the ADIOS system. It is used to capture interest in Network events such as route requests, route responses and random transactions by a temporary neighbor for consideration.

5) Multiple Voting System: Multiple voting system is in part aimed at reducing attacks on a given network as it makes the final decision to split whether a node is black or not on the basis of a multi-system system.

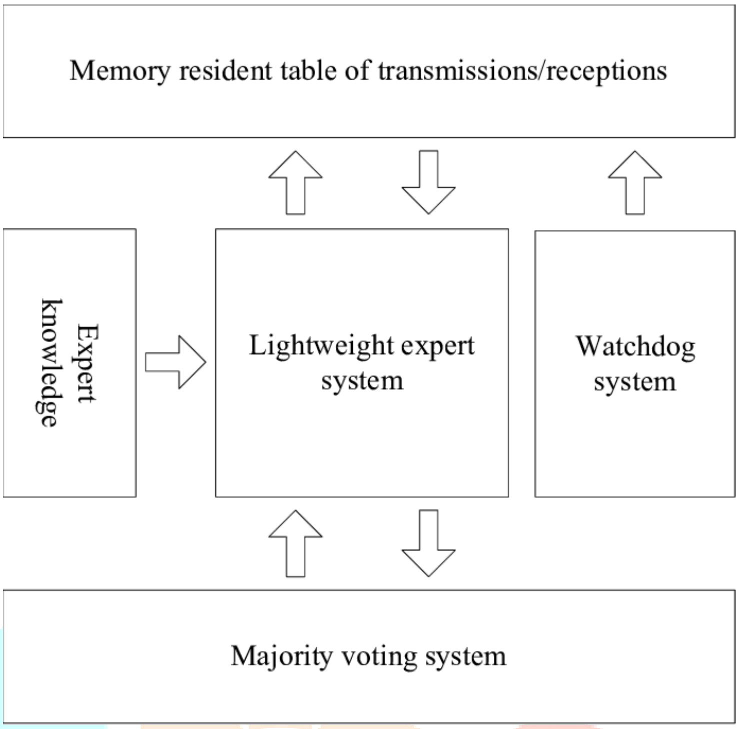
Memory resident table of transmissions/receptions
Expert knowledge
Lightweight expert system
Watchdog system
Majority voting system

Figure 6. ADIOS building diagram

B. How to Attack

Our approach to attack detection is using ADIOS resolution in relation to its implementation of various communication layers. These are the following:

1) Detection of Invalid Node in MAC Layer: Media Access Control Agreements (MAC) are specifically designed for WSN to reduce Power consumption and monitor the limitations of their Processors. There are two main categories of MAC protocols for WSNs based on how the MAC controls when certain nodes are able to communicate in a channel namely Time Division Multiple Access of companies that carry stakeholders and retreat. to avoid collisions). Malicious Node detection in the MAC Layer is based on the concept of hop-count value relative to the fixed value of the black process detection and blocking separately by blacklisting a black node and removing it from the network.

2) Negative Node Discovery on the Layer Network: The work layer on the ad-hoc wireless network is concerned with neighborhood acquisition, traffic distribution, and distribution of powerful resources. An important variation in the route used by sensory networks is network processing such as data integration and filtering unwanted information.

The process used for Malicious node detection and blocking in Network Layer is based on the concept of algorithm for selecting the path, stability and loading of the network and as a result the attacker node is called Red and removed from the network.

3) Physical Layer Invalid Node Detection: The natural layer in WSNs works with the flexibility and minimization of digital data, which means data transfer and acceptance. It is made up of transceivers present in sensory nodes. The main functions of the body layer are to select the network company and production frequency, encryption and encryption, voice fluctuations and to remove physical degradation, transfer and acceptance of data in the network system

.

The concept of acquiring and reducing access to Physical Layer is based on the concept of network-related transmission power and distance between the sender and receiver and as a result the Black node is detected in the network system.

IV. RESULTS OF SIMULATION AND ANALYSIS

The simulation results show us how well the proposed system works in real life situations and help us to understand it easily using graphs. To simulate the performance of each node that monitors a random set of network events, a network traffic is generated that contains black hole attacks.

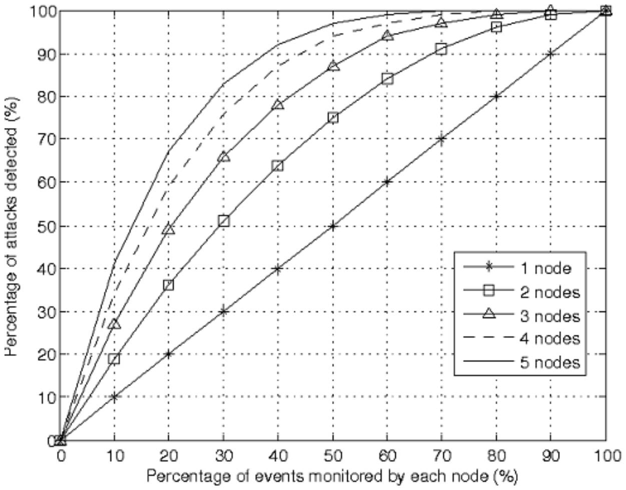

Figure 7. Per. Attack found vs Per. of supervised events

Also, the attack took place throughout the vehicle dump and the nodes were instructed to look only at random parts of this traffic and report any irregularities. Number of nodes in location and number of attacks

they varied between these imitations. This simulation was performed 1000 times taking measurements using Per. Attack found vs Per. of supervised events. The more powerful nodes, the greater the chances of getting an attack and where the network will live longer to perform its application functions.

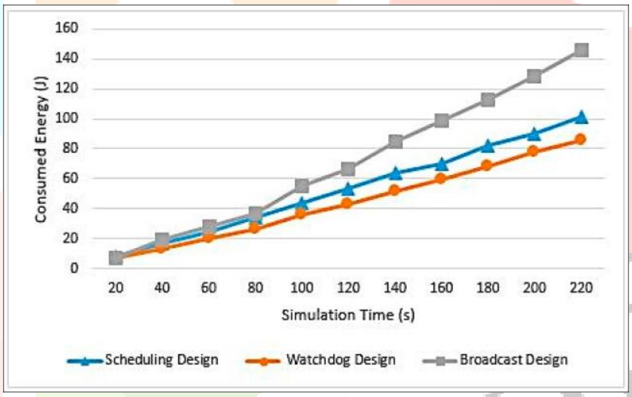

Fig. 8. Energy consumption measurements

The Watchdog project uses very little power among other projects due to its monitoring system which reduces the amount of messaging required and therefore reduces energy costs and increases the time at which the network can operate efficiently.

V. CONCLUSION

In this project, we aimed to improve the Intrusion Detec- System for ad-hoc networks that detect black hole attacks on Wireless Sensor Networks using an Expert System that works on various components such as MAC Layer, Physical Layer and Network Layer. We described the development of such a system and called it the ADIOS System and tried to measure the performance and use of resources because it is important in the case of WSNs. Using simulation, we have also shown that we can detect the fact that multiple nodes in the network reduce the processing, memory and battery life of each node while maintaining the ability to detect accurate attacks.

As a future work, a variety of approaches can be developed and implemented to reduce resource utilization and code to improve and improve and ensure the delivery of high-quality packages between locations. Also, this algorithmic program can be used with specific learning algorithms such as segmentation to make it dynamic and flexible with great efficiency working for real world advanced applications.

REFERENCES

[1] Shaveta, Pawan Luthra, Er. Gagandeep" Implementation of blackhole attack under aodv routing protocol", Chennai, India, IEEE, 2017

[2] Taylor Vincent F, Fokum Daniel T" Mitigating Black Hole Attacks in Wireless Sensor Networks Using Node Resident Expert Systems", Washington, DC, pp.1-7, IEEE,2014.

[3] Abhinav Kaurav, Kakelli Anil Kumar Detection and Prevention of Blackhole Attack in Wireless Sensor Network Using Ns-2.35 Simula- tor" International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2017.

[4] Abdullah Aljumah, Tariq Ahamed Ahanger" Futuristic Method to Detect and Prevent Blackhole Attack in Wireless Sensor Networks".

[5] Hanane Kalkhaa,Hassan, Satori, Khalid Satori "Preventing Black Hole Attack in Wireless Sensor Network Using HMM"

[6] Maryam Motamedi,Nasser Yazdani "Detection of Black Hole Attack in Wireless Sensor Network Using UAV "

[7] Yingpei Zeng, Jiannong Cao, Shigeng Zhang, ShanqingGuo, Li Xie" Random-walk based approach to detect clone attacks in wireless sensor networks"

[8] Nitin A. Sakhare, Nilesh U. Sambhe" DETECTION OF MALICIOUS NODE BY BLACK HOLE ATTACK IN WIRELESS SENSOR NET- WORK BASED ON DATA MINING"

[9] Shalu Malik, Dr. Anil Kumar Sharma" DETECTION AND ISOLATION TECHNIQUE FOR BLACKHOLE ATTACK IN WIRELESS SENSOR NETWORK"

[10] Samir Athmani, Djallel Eddine Boubiche, Azeddine Bilami" Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs"

[11] Er. Amandeep Kaur, Er. Parveen Kaur, C. Er. Harisharan Aggarwal" Intrusion Detection System (IDS) for Black hole attacks- A Literature"