Journal of Computing Research and Innovation (JCRINN) Vol. 6 No. 2 (2021) (pp173-181)
https://jcrinn.com : eISSN: 2600-8793

Sinkhole Attack in IDS: Detection and Performance Analysis for Agriculture-based WSN using Cooja Network Simulator

Iman Hazwam Abd Halim[1]*, Mohamad Hafiz Abdul Azziz[2], Mohd Faris Mohd Fuzi[3]
[1,2,3] Faculty of Computer and Mathematical Sciences,
Universiti Teknologi MARA, Perlis Branch, Arau Campus, 02600 Arau, Perlis, Malaysia

*Corresponding author: * hazwam688@uitm.edu.my*
Received Date: 15 August 2021
Accepted Date: 21 August 2021
Published Date: 1 September 2021

HIGHLIGHTS

- Agriculture-based WSN is one of the areas that was harmed with the DDoS attack.
- Sinkhole attack is the most common to happen in any WSN environment.
- IDS was introduced and implemented to help from being hijacked by the attacker.
- Cooja Network Simulator can be used to simulate the IDS testing.

ABSTRACT

Wireless Sensor Network (WSN) takes a major part in the world of technology and everyday lives by implementing Internet of Things (IoT) sensors into many kinds of environment such as agricultural area. Many farmers had applied WSN to help them to ease the tasks of tracking and collecting the important data status of their farms and greenhouses in order to maintain its ideal temperature, humidity and lights exposure. Despite these advantages, the WSN security issues could be questioned due to the possibility of being infected by the Distributed Denial of Service (DDoS) from the attackers. Sinkhole attack is the most common DDoS attack that happened in the agriculture environment WSN by sending a fake fastest route to the sensor nodes in the system. Therefore, this project has proposed an Intrusion Detection System (IDS) to detect the sinkhole attacks in the network of agriculture based WSN. The project ran with three simulations of network topologies to show the comparison based on the network traffic performance. The simulations consist of attack-free network, a network with sinkhole attack and IDS in the malicious sinkhole network. The main simulator for the study was Cooja Network Simulator, which was used to conduct all three simulations, while Wireshark was utilised to capture network traffic performance. For every simulation, 20 sensor nodes were implemented due to the facts that the number of the nodes are majorly and ideally used in real life environment of agriculture area. The findings showed that by implementing IDS in the agriculture WSN will gives better results in network traffic performances comparing to the attack-free network and sinkhole network without IDS. Thus, it proved that the proposed IDS could detect the network when uncommon behaviour appeared in the network topologies.

Keywords: *Sinkhole attack, Intrusion Detection System (IDS), Wireless Sensor Network (WSN), Cooja Network Simulator*

INTRODUCTION

Wireless Sensor Networks (WSNs) is undoubtedly one of the most needed things the world cannot live by due to its durability, cost-effectiveness, subtle elements and smart sensor nodes. WSN also applied in many kinds of environment applications such as health medical monitoring, battlefield surveillance, home environment, agriculture and other commercial areas. The sensor networks have helped a lot of people in many areas by minimizing their works and make the duties go a lot faster than before.

Meanwhile, this project was focused on the agriculture environment because it is one of the most anticipated area in WSN. Since the WSN was introduced in this area, farmers have taken a lot of interest in applying the sensors to help them to minimize their work like monitoring the temperature for plants to grow healthy and not dying. The sensors could also be applied for animals in the farms such as cows and chicken. The sensors could be used for detecting the health and the behaviour of farm animals thus, alert the farmers if detected any unusual activities, such as disease and animal infections.

Despite many advantages that can be gained in this area by implementing WSN, the network in agriculture-based also vulnerable to attacks. The attackers will inject the Distributed Denial of Service (DDoS) attacks which include harm and make the network ineffective to communicate. One of DDoS attack that commonly used by the attacker to destroy the WSN of agricultural area is sinkhole attack. The fake node then, notify the neighbouring nodes as the quickest routes to the base station and thus trick the nodes into giving the information in the WSN (Ali, Nadeem, Siddique, Ahmad & Ijaz, 2020).

To prevent more of this attack occurred in the future of agriculture-based WSN, this project introduced the Intrusion Detection System (IDS) to detect the sinkhole attack. The IDS identify inconsistencies and classifies them as attempts to breach security objectives such as confidentiality and integrity in a computer information system, a network, or a cloud computer (Lakshminarayana, Philips & Tabrizi, 2019). By implementing IDS in the system, the network security of the agriculture topology will be improved.

In the previous work, many researchers also discovered a lot of security protection method into the WSN using simulations. Firstly, Arora, Vijan & Goba (2018) have implemented Ad-hoc On-demand Distance Vector (AODV) routing protocol to prevent Packet Delivery Ratio (PDR) loss. Meanwhile, the watchdog mechanism by Stephen & Arockiam (2017) to detect the sinkhole attack in IoT environment by using the Tetcos NetSim.

Since the project also ran using simulations, the network simulator that was used is named Cooja of Contiki Operating System (OS). This simulator could be found online and downloaded using the web browser, after that ran inside the VMware Workstation Pro to access the operating system and its features.

In the next section, the methodology of project planning and development were discussed in details for setting up the network topologies, sinkhole attack and IDS. The results were shown later in the findings and discussions section after completing the project thus led to the conclusion section.

METHODOLOGY

This project adapted the waterfall model for the methodology. The methodology included information gathering to identify the requirement needed and what to collect based on the project's objectives. Next was the planning phase which was to identify the hardware and the software that would be used. For the network designing phase, the network topologies were created to be used to run the simulations. In the simulation testing phase, there were three simulations that need to be implemented which were; 1. An

attack-free simulation, 2. A network with sinkhole attack, 3. A network with sinkhole attack and IDS. This to align with the objectives of the project which was to prove that implementing IDS in the network with sinkhole attack can help the farmers' data be protected, and also, to compare and investigate the network traffic of the system as well as the network attribute behaviour of both sinkhole attack and IDS. The fifth step was to record the data in the data analysis phase. The outputs concluded were the routing metric, data packet captured using Wireshark and the sensors monitoring. For the last phase, the results were compiled and documented in a single report thus completing the purpose of this project.

Simulation Parameter

The OS that was used is Contiki-3.0 OS which is an open source OS that makes used Linux Ubuntu 14.04 Long Term Support (LTS) and can be downloaded from any browser. VMware virtual machine is needed to run Contiki OS. Cooja is a network simulator that allows you to emulate real-world hardware platforms and also, an application that focuses on network behaviour with its functionality to run IoT based smart devices in simulations. Mote is another name for the sensor node used in the Cooja Network Simulator. As cited by Deshmukh-Bhosale and Sonavane (2019), the ideal number of sensor nodes to be used in agricultural environments such as greenhouse, are 20 nodes meanwhile, the ideal simulation area for a greenhouse is 30x35 meters. Table 1 below indicates the simulation parameter to be used in this project.

Table 1: Simulation parameter

Parameter	Value
Simulator	Cooja Network Simulator
Number of nodes (motes)	20
Simulation area (meters)	30x35
Simulation time (seconds)	600
Mote start-up delay (seconds)	1
Default mote used	Tmote Sky
Packet size (bytes)	512
Topology	Linear Positioning

The simulation area mentioned in the Table 1 above used the exact parameter of a real-life greenhouse, which was also one of the environmental based of agriculture. Figure 1 below indicated a greenhouse planning sketch that was used as the model for this project with the Internet of Things (IoT) sensors in it.

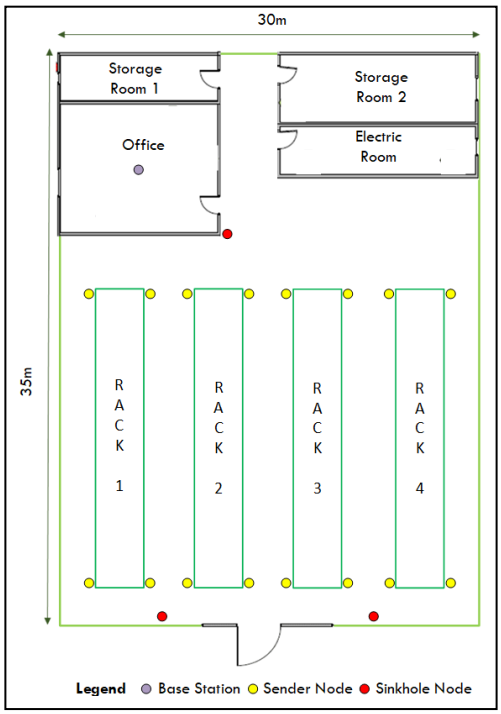


Figure 1: A greenhouse planning sketch with the IoT sensor nodes

Simulation Topologies

There were three simulations that were held for this project as mentioned before in the methodology. Figure 2 below showed the motes used in the attack-free simulation were all the same because there were no attack available. In Figure 3, there were 17 normal motes and three sink motes to establish the sinkhole attack simulation. Lastly in Figure 4, there were 13 normal motes, 3 sink motes, and four IDS motes in the topology to run the sinkhole attack simulation with IDS protection.

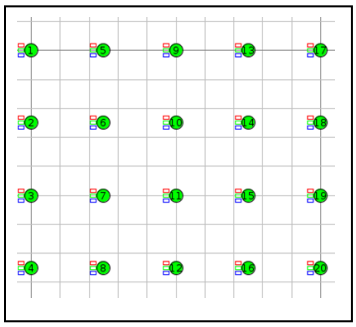


Figure 2: Attack-free simulation

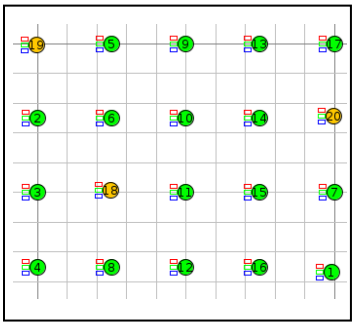


Figure 3: Simulation with sinkhole attack

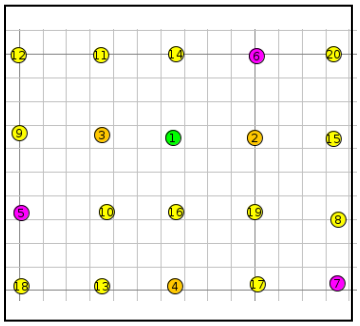


Figure 4: Sinkhole attack simulation with IDS

Simulation Scripting

This simulator runs C# script while the interface runs using Java programming language. The scripts were already included inside the OS and can be run for each simulation. The scripts that were used for this project are as shown below in the Table 2.

Table 2: Scripts used in each simulation

Simulation	Scripts used
1	collect-view-shell.c
2	udp-sender.c
	udp-sink.c
3	udp-sender.c
	udp-sink.c
	border-router.c
	sky-websense.c

For the first simulation, the script that were used to easily collect the data without any attack was the collect-view-shell.c. The second simulation used two scripts which were, the udp-sender.c and the udp-sink.c. The first script in the second simulation was modified from the first simulation to combine and work with the udp-sink script which would act as the sinkhole motes inside the simulation. And lastly for the third simulation, there were another two scripts that would be added which were the border-router.c and sky-websense.c to make the nodes connect into the router and the Internet. These scripts could also be an IDS for the system and that was how the sinkhole network with IDS protection was simulated.

FINDINGS AND DISCUSSIONS

There were three results that could be concluded from this project as mentioned previously in the methodology. The first one was the sensors monitoring to prove that the sensors were working perfectly fine during all simulation test runs. The second result was the routing metric which was to compare the most rejecting and selecting routes for every simulation in the project. The most ideal selecting route was the best choice for the farmers to use in their agricultural-based WSN. Lastly, the data packet captured by using Wireshark to show the network behaviour of each simulations and decide which was the better one.

Sensors monitoring

The most common used sensors in agriculture-based WSN environment were light sensor, temperature sensor and humidity sensor. The monitored sensors showed the same output results in all three simulations to prove that the sensors were working perfectly fine in any kind of phenomena. Below were the figures of the sensors monitoring that have been collected using the Sensor Data Collect with Contiki window after running the simulations for 600 seconds.

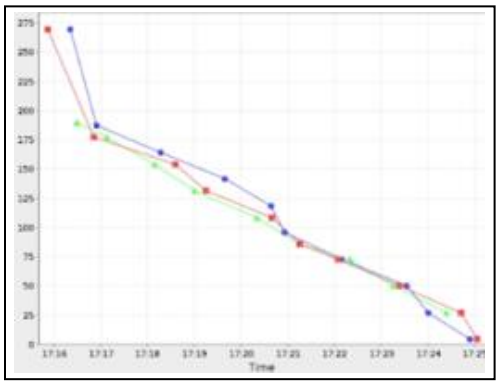


Figure 5: Light sensor

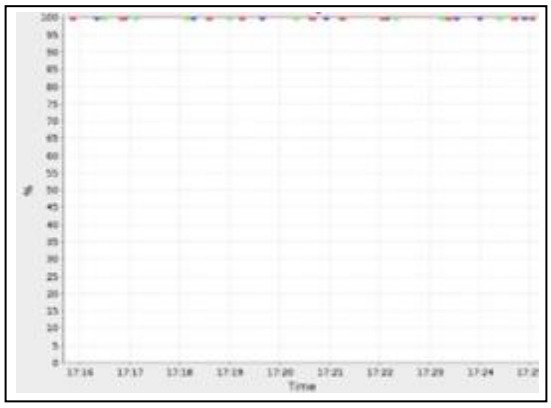


Figure 6: Humidity sensor

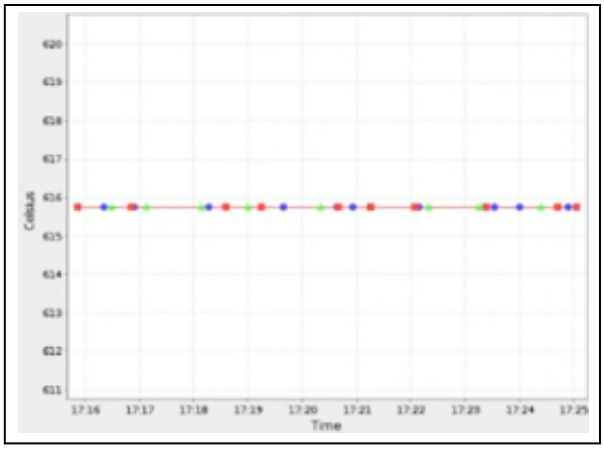


Figure 7: Temperature sensor

Figure 5 showed the light sensor graph was decreasing to show the amount used in all simulations. When needed, the line will go up and thus repeat again. Meanwhile, Figure 6 indicated the humidity which showed at the peak of 100%. This showed that the humidity was great and can be used to implement in agricultural area. Lastly for temperature sensor in Figure 7, the line graph above shows the sensors were at the optimum value in the simulation processes.

Routing Metric

This comparison the routing metric was for selecting or rejecting a routing path for transferring data packets by the sensor motes in Cooja by a routing algorithm. Metrics were assigned to each different route available in the routing table for optimal route to send a data packet from one mote to another.

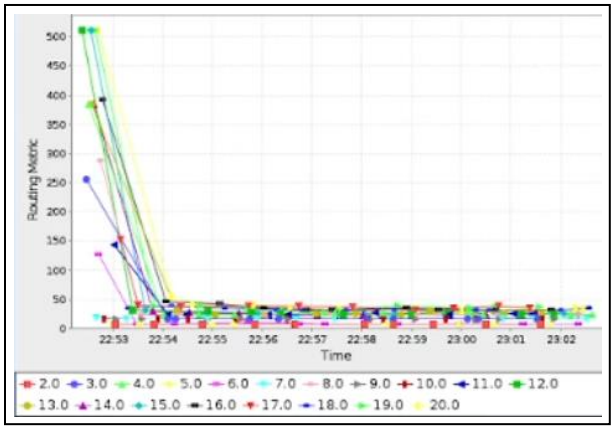


Figure 8: Routing metric in the first simulation

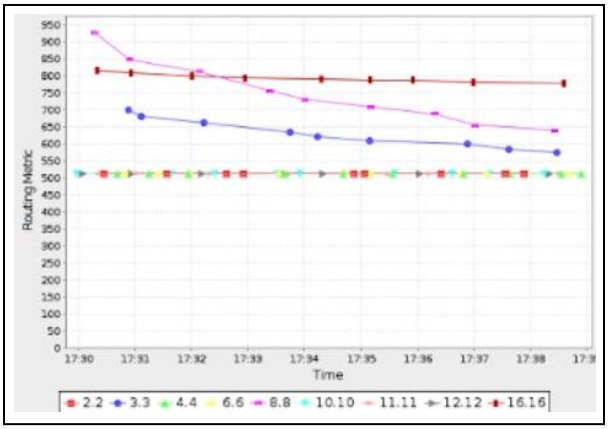


Figure 9: Routing metric in the second simulation

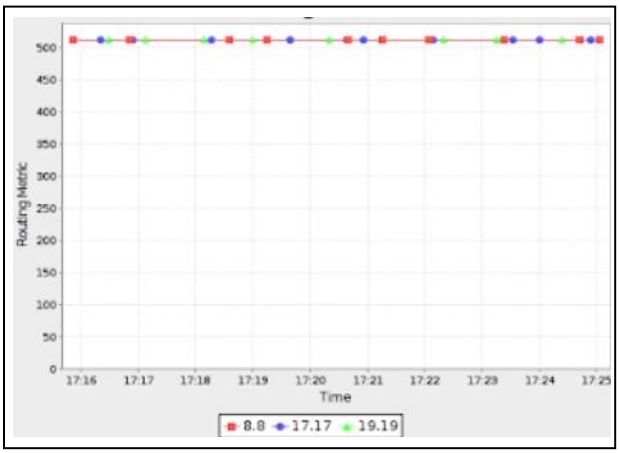
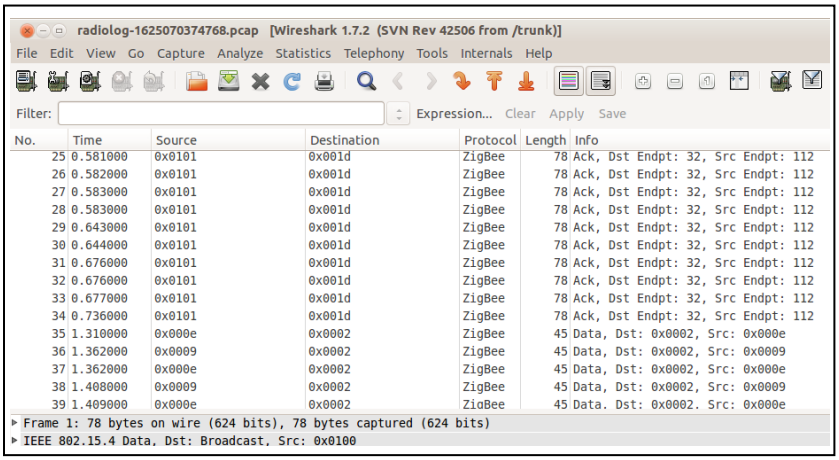


Figure 10: Routing metric in the third simulation

Figure 8 showed the results for routing metric in the first simulation with 500 routing peaks until the lowest number in the graph. Figure 9 with the sink motes available in the topology indicated the different graph from the previous simulation due to difference in scripting. Some of the motes have ideal position of graph by maintaining its routing metric. The pink, red and blue line which were mote 2,3 and 8, were not in the ideal line because they use more routing metrics to fight back the interception of the sinkhole attack. This means that those three motes in the figure data have been hijacked by the attacker using the sink motes in the network. In the third simulation of Figure 10, IDS sensor motes have been inserted to make sure the routing metrics and shows a better result from the second simulation.

Data packet captured by Wireshark

Wireshark was chosen as the application that can captured the data packet sends by the sensors during all simulations to prove the network is being intercepted by the attacker. The radio log of the simulations can be found in *contiki/tools/cooja/build* folder.



Neither sinkhole attack nor IDS were available in this simulation.

Figure 11: Wireshark analysis for the first simulation

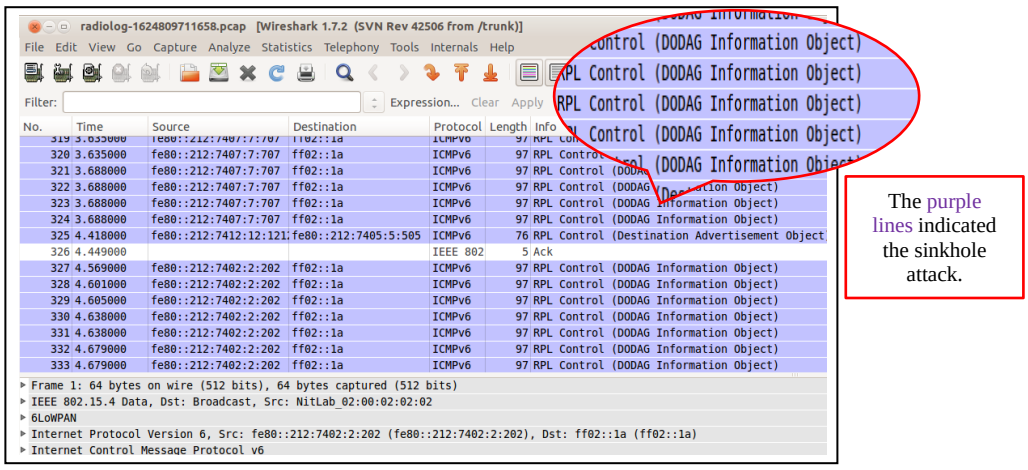


Figure 12: Wireshark analysis for the second simulation

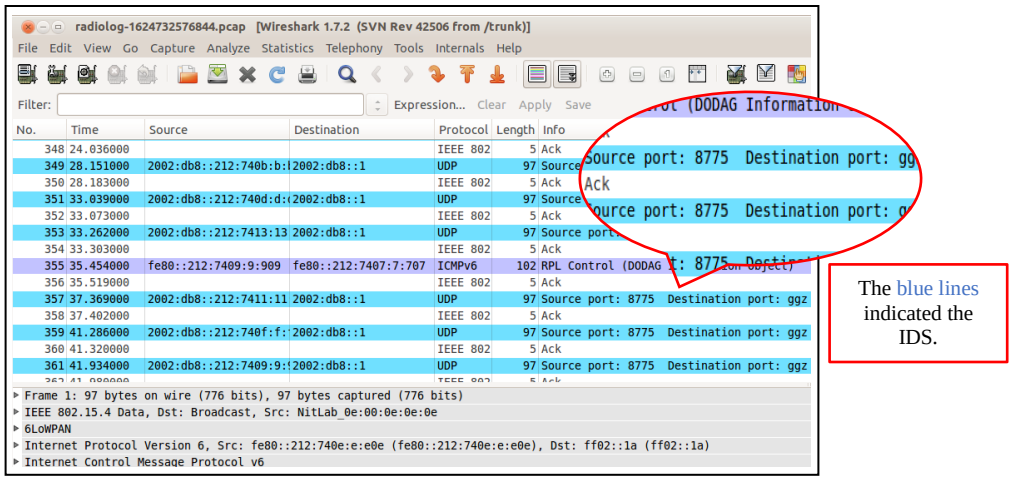


Figure 13: Wireshark analysis for the third simulation

Figure 11 showed all sensors in the first simulation can send data packet to the BS safely as there were no sinkhole motes available in the network. Unfortunately, in Figure 12, there were a lot of purple lines and most of them wrote RPL Contract (DODAG Information Object) which indicates the sinkhole attack happening in the network. This was not a safe network for the farmers because the attacker may steal the data or even worse, drop the data packet before it even reach the BS. To avoid losing any data packet to the sink motes, Figure 13 showed the safest network with blue line of IDS that implemented using the RPL Border Router script and IPv6 through to the Internet.

CONCLUSION AND RECOMMENDATIONS

The Sinkhole Attack Detection using IDS was developed for farmers of the agricultural environment that uses WSN in order to give security to their network system. This project was successful because both objectives have been achieved and can be proven to the farmers who use WSN in their agriculture that IDS

was a better security to protect the sensors from being hijacked by the attackers than the network without any attack or network with sinkhole attack in it.

There were many limitations that can be found during the project's development. The first limitation of the project was that it could only detect the attack that being intercepted by the attacker in the WSN instead of preventing it. The second limitation that could be found in this project was the difficulty in modifying the scripts of IDS to make an enhanced version from the available scripts inside Contiki OS. It was not easy to modify and to add new command in the scripts because it will create too many errors thus, the project cannot be completed.

As there are limitations to the project, there were also some ideas for future researches and studies which can be implemented in the future such as upgraded the security level by implementing Intrusion Prevention System (IPS) into the topologies to detect and then prevent the attack from getting any worse for the farmers with WSNs technology. Apart from that, future researchers may try to implement other DDoS attacks into the simulations of agriculture to identify how the attacks will behave in the network and how IDS can prevent those malicious nodes.

REFERENCES

Ali, M., Nadeem, M., Siddique, A., Ahmad, S., & Ijaz, A. (2020). Addressing Sinkhole Attacks in Wireless Sensor Networks - A Review. International Journal of Scientific and Technology Research (IJSTR), 9(08).

Arora, S. K., Vijan, S., & Gaba, G. S. (2016). Detection and analysis of black hole attack using IDS. Indian Journal of Science and Technology, 9(20). Retrieved from https://doi.org/10.17485/ijst/2016/v9i20/85588

Deshmukh-Bhosale, S., & Sonavane, S. S. (2019). A Real-Time Intrusion Detection System for Wormhole Attack in the RPL based Internet of Things. In Procedia Manufacturing (Vol. 32, pp. 840–847). Elsevier B.V. https://doi.org/10.1016/j.promfg.2019.02.292

Lakshminarayana, D. H., Philips, J., & Tabrizi, N. (2019). A survey of intrusion detection techniques. In Proceedings - 18th IEEE International Conference on Machine Learning and Applications, ICMLA 2019 (pp. 1122–1129). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICMLA.2019.00187

Stephen, R., & Arockiam, L. (2017). An Enhanced Technique to Detect Sinkhole Attack in Internet of Things. International Journal of Engineering Research & Technology (IJERT) ICONNECT – 2017 (Volume 5 – Issue 13). Retrieved from https://www.ijert.org/an-enhanced-technique-to-detect-sinkhole-attack-in-internet-of-things