DETECTION AND PREVENTION OF BLACK HOLE ATTACK IN WIRELESS SENSOR NETWORK

Stella K
Department of Electronics and Communication Engineering
Veltech Hightech Dr.Rangarajan Dr.Sakunthal Engineering College
Chennai, India
stellaakk16@gmail.com

K Thamizh Azhagan
Department of Electronics and Communication Engineering
Veltech Hightech Dr.Rangarajan Dr.Sakunthala Engineering College
Chennai, India
tamilecesec@gmail.com

Suhail Akthar
Department of Electronics and Communication Engineering
Veltech Hightech Dr.Rangarajan Dr.Sakunthala Engineering College
Chennai, India
zuhailakthar@gmail.com

P chandru
Department of Electronics and Communication Engineering
Veltech Hightech Dr.Rangarajan Dr.Sakunthal Engineering College
Chennai, India
c6383158906@gmail.com

MD Faheem
Department of Electronics and Communication Engineering
Veltech Hightech Dr.Rangarajan Dr.Sakunthala Engineering College
Chennai, India
faheemhaker@gmail.com

Abstract—In this research, we investigate how to recognise and stop black hole attacks in networks of sensors. A sensor network that is wireless is a device that combines software, gateways, and devices known as sensor nodes. These wireless network nodes have the ability to send data to other nodes. It is crucial to numerous applications, including those in the military, medical field, transportation, industry, and agriculture, among others. The networks of wireless sensors, or WSNs, are susceptible to a variety of security flaws, including black hole, message replay or manipulation, identity spoofing, and wormhole threats. Hackers that target a node to turn it into a hostile node that will provide the recipient with misleading information are committing a black hole attack. These nodes with wireless sensors (WSN nodes) have short battery life and storage capacity, restricted processing speed, and limited transmission range in the Internet of Everything. These days, a vast number of networks are used in commercial, industrial, and healthcare settings. Instead of sending accurate information to the station, the intermediate captures and reprogrammes a group of nodes to block packets and generate bogus signals when it detects black. In this article, we specifically address the detection and mitigation of black hole attacks in networks of wireless sensors. Provide complex defenses against threats from black holes as well. Additionally, a trust-based method for detecting Black hole threats was presented. The NS-2 simulator uses the simulation results, which are assessed in terms of packets. By analyzing using an NS-2 emulator, malicious nodes may be prevented from accessing wireless networks, and steps can be taken to lessen the impact of network attacks.

Keywords— Wireless sensor network, Black hole attack, Security, AODV, Route security protocol

I. INTRODUCTION

Wireless Sensor Network (WSN) is an infrastructure-less wireless network that is deployed in a large number of wireless sensors in an ad-hoc manner that is used to monitor the system, physical or environmental conditions. Sensor nodes are used in WSN with the onboard processor that manages and monitors the environment in a particular area. They are connected to the Base Station which acts as a processing unit in the WSN System. Base Station in a WSN System is connected through the Internet to share data.Typically, a wireless sensor node (or simply sensor node) consists of sensing, computing, communication, actuation, and power components.These components are integrated on a single or multiple boards, and packaged in a few cubic inches.In many applications, wireless sensor networks often operate in hostile and unattended environments. Therefore, there is a strong need for protecting sensing data and sensing reading from various attacks like sinkhole attack, blackhole attack, etc. The proposed approach provides a solution to meet sinkhole attack.A Wireless Sensor Network is a network of spatially distributed sensors that monitor physical or environmental conditions and communicate their data to a central location.

WSNs are widely used in various applications such as environmental monitoring, healthcare, military, and industrial automation.A black hole attack is a security threat in WSN where a compromised or malicious node

falsely claims to have the shortest path to the sink node (central node) and absorbs all the incoming data packets. Instead of forwarding the data to the sink, the black hole node drops or manipulates the packets, leading to data loss and disruption in the network.The majority of wsn is in biggest threat in this gen-z world(generation) as everything now is based on cloud and wire-less sensor networking.

II. RELATED WORKS

The paper [1]: the author discusses A wireless sensor network consists of small, low-power sensor nodes deployed to monitor physical or environmental conditions, often relying on batteries for energy. While these networks are versatile, their lack of infrastructure makes them vulnerable to security threats, such as the Wormhole Attack, where an attacker creates a tunnel between distant locations to manipulate communications without disrupting the network structure. [2]has described A Wireless Sensor Network (WSN) is a bunch of closely placed sensor nodes that keep an eye on different things. Thanks to advancements in technology, these nodes are now smaller, cheaper, and use less power. Each sensor node has its own resources like energy, wireless communication, and Micro Electro Mechanical Systems (MEMS). WSNs are used in various areas like military activities, environmental monitoring, healthcare, industrial processes, and urban surveillance.[3] has described In the network layer, some sensors may get compromised and mess with the routes, controlling how information flows. This poses a threat to the network's integrity. The paper is organized into sections discussing attacks, related work, the proposed system, simulation results, and conclusions. [4]This research focuses on enhancing energy-aware routing and detecting black hole attacks in Wireless Sensor Networks (WSN) using a deep-stacked autoencoder. The proposed approach involves energy-aware routing based on parameters like energy, distance, and delay, followed by black hole attack detection at the WSN base station using a pre-processed data-driven method.

[5]The author discusses Black Hole (BH) attacks in wireless sensor networks (WSNs), where malicious nodes advertise false paths to attract traffic but drop the packets instead of forwarding them, causing a denial-of-service (DoS) effect. These attacks significantly degrade network performance, impacting throughput, end- to-end delay, and energy consumption of nodes. The limited resources in WSNs make them vulnerable to such security threats. The paper explores the challenges posed by BH attacks, emphasizing their classification into single and collaborative attacks, which are harder to detect and more detrimental to network performance.

[6] these author says In practical applications like battlefield surveillance and forest fire detection using wireless sensor networks (WSNs), nodes are densely and randomly deployed in hazardous conditions to monitor events collaboratively. However, the wireless communication and unattended deployment make the network susceptible to node capture attacks, where a sensor node is physically obtained, reprogrammed, and redeployed for malicious purposes. Detecting such attacks remains challenging due to potential false reports from non-captured malicious nodes and the limitations of existing detection protocols.The challenge lies in developing effective protocols for detecting and preventing node capture attacks in WSNs, considering the resource constraints of sensor nodes and the risk of malicious collaboration among network nodes.

[7]This research addresses security concerns in Wireless Sensor Networks (WSN), focusing on detecting Gray Hole attacks and implementing an Enhanced Adaptive Acknowledgment (EAACK) scheme. Gray Hole attacks occur when nodes falsely claim to forward data but disrupt communication, impacting the Ad-hoc On- demand Distance Vector (AODV) routing protocol.

[8]SARITA AGRAWAL , MANIK LAL AND JAVIER LOPEZ[2017] Detection of Node Capture Attack in Wireless Sensor Networks. Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Network. DHARA BUCH,D. C found Denial of Service Attacks in Wireless Sensor Networks. MANDEEP KUMAR AND JAHID ALI[2022] Taylor Sailfish Optimizer-Based Deep Stack Auto Encoder for Blackhole Attack Detection in Wireless Sensor Network MISS.
]PRACHI S. MOON MR. PIYUSH K. INGOLE[2015] An Overview on: Intrusion Detection System with Secure Hybrid Mechanism in Wireless Sensor Network.[9] [10][11]

ASHISH JAIN MADHU SHARMA[2016] Wormhole Attack in Mobile Ad-hoc Networks. [13]Abdulmalik Danmallam Bello, Dr. O. S. Lamba, 2020, How to Detect andMitigate Sinkhole Attack in Wireless Sensor Network International Journalof Engineering Research & Technology (IJERT) Volume 09, Issue 05 Semagn Shifere et al. Department of Computer Science Woldia University, Ethiopia ,Volume 6, Issue 2, February – 2021 International Journal of Innovative Science and Research Technology ISSN No:-2456-2165.

[14]Sihem Aissaoui & Sofiane Boukli, Sinkhole attack detection based on SVM in wireless sensor network, international journal of wireless networks and broadcast technologies,IGI Global, vol. 10(2), pages 16-31, July.
Neha Singh, Kamakshi Rautela [2016], International Journal of Engineering and Computer Science ISSN: 2319 – 7242, Volume 5, pp. no. 17544-17548.

[15]Dhivya M et al. vol.2, 2021, Detection and Prevention of Sinkhole Attack inWireless Sensor Network using Armstrong 16-digit Key Identity and GANNetwork.

[16]Sumit Pundir et al. [2020] designed efficient sinkhole attack detectionmechanism in egde based IoT deployment
2017, pp. 359–365, doi: 10.1109/CESYS.2017.8321299. 15. K. Karthigadevi and M. Venkatesulu, “Based on Neighbor Density Estimation Technique to Improve the Quality of Service and to detect and Prevent the Sinkhole Attack in Wireless Sensor Network,” 2019 IEEE International Conference on Intelligent Techniques in the control, Optimization and Signal Processing (INCOS), Tamilnadu, India, 2019, pp. 1–4. 16. Vidhya, S, “Sinkhole Attack Detection in WSN using Pure MD5 Algorithm.” Indian Journal of Science and Technology 10.24 (2017).

BLACK HOLE ATTACK IN WIRELESS SENSOR NETWORK

1. WSN Architecture:~

A base station, clusters, and sensor nodes make up the architecture of a network of wireless sensors connected to the internet, can communicate with the base station.

2. WSN Architecture:~

A base station, clusters, and sensor nodes make up the architecture of a network of wireless sensors (WSN). Computers at different places, such an end-user terminal connected to the internet, can communicate with the base station.

\

2. BASE STATION:~

A base station consists of the antennas and other equipment needed to connect wireless communications devices to the network. It will reflect as an entry to other networks through the web source.

3.CLUSTERED NETWORK ARCHITECTURE:~

A two-tier hierarchy clustering architecture is a clustered architecture network. Sensor nodes are grouped together into units known as clusters which gives a distributed approach.

4.SENSOR NODES:~

A network gateway receives the data from sensor nodes in a network of wireless sensors (WSN) that detect environmental factors. After that, the data is compiled, stored, and processed by the gateway.

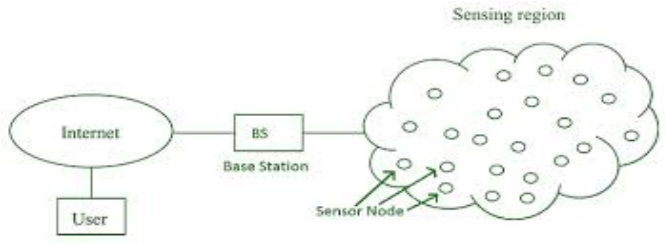


figure 1.1

A.WSN Characteristics:~

A network of wireless sensor (WSN) is a platform that connects many distributed sensors. WSNs have several characteristics, including: Power consumption: WSNs have limitations on how much power sensor nodes can consume. Node failures: WSNs can handle node failures. Node mobility: WSNs have mobile nodes. Large-scale deployment: WSNs can be deployed on a large scale. Environmental conditions: WSNs can survive harsh environmental conditions. Scalability: WSNs are flexible and scalable, allowing for easy deployment and reconfiguration of sensor nodes. Localization: WSNs use localization to identify the location of sensor nodes. Quality of service: WSNs provide high accuracy in data delivered to central control. Security: WSNs have limited security, as nodes can be intercepted, jammed, and seized.ROBUST OPERATIONS: Since the sensor nodes are deployed in hostile environments, they have certain capability of fault and error tolerance. Therefore, it is necessary to develop ability of sensor nodes in terms of self-test, self-calibrate and self-repair.The major concerns in wireless sensor network is security. There are quite prone to unlicenced access, attack,unintentional issues on the information inside of the node. The next part mainly focuses on sinkhole attack.

B. WSN SECURITY THREATS :~

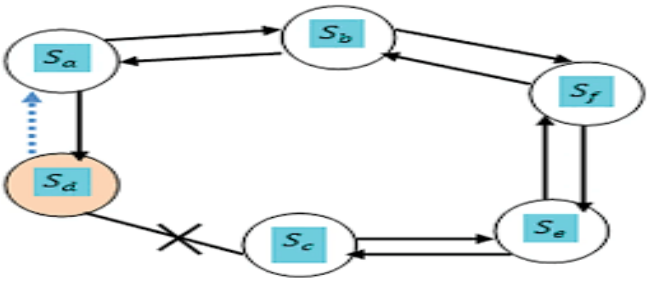
There are various threats in wireless sensor networks as it includes packages which that contains important and secured files. The informations are not only to be stolen but can also be manipulating the information of the particularfile.

- SELECTIVE FORWARDING
- MANIPULATING ROUTING
- INFORMATION
- SINK HOLE ATTACKS
- WARMHOLE ATTACKS
- BLACKHOLE ATTACKS
- DENIAL OF SERVICE

Black Hole Attack Detection

1.INTRODUCTION :~

Wireless Sensor Networks (WSNs) have emerged as a critical technology, enabling efficient monitoring and data collection in various domains, from environmental sensing to healthcare. However, within the realm of WSNs, a lurking threat known as the "Black Hole" has become a significant concern. Similar to its cosmic counterpart, the Black Hole in WSNs represents a malicious entity capable of disrupting communication and compromising the integrity of the network.



Black hole detection diagramaic view

PROPOSED METHOD AND SYSTEM

ARCHITECTURE

1.WATCHDOG MECHANISM:

In a Watchdog-based approach, each node monitors the behavior of its neighbors.Nodes (watchdogs) check if their neighboring nodes are forwarding the data packets they claim to receive.If a node is detected as a potential black hole, it can be isolated, and alternative paths can be explored. Nodes continuously monitor the behavior of their neighbors.

2.. AODV ROUTING PROTOCOLS:

Ad hoc networks use ADOBE , a loop-free protocol . Designed to be proactive in a mobile node environment and

able to tolerate a range of behaviors, including packet loss, connection failures, and node mobility.AODV is an on-demand algorithm, meaning that it builds routes between nodes only as desired by source nodes.

It maintains these routes as long as they are needed by the sources.The figure 4.1 explains the aodv(Ad hoc On-Demand Distance Vector) process as the source uses the rreq(route request) on its neighboring node to confirm the behaviors of that specific node. The corresponding node will give rrep(route reply)as a response.

This process continues until the source reaches its destination.Route Request, or RREQ, is a term used in Sensor Networks contexts. A link to the AODV routing protocol. When a WSN node moves data to packets to a designated end.When a node finds itself without a route to it, it starts the Route Discovery procedure.

Until it reaches the final node or comes across a node with a useful path to the intended destination, the FREQ propagates throughout the network.

The performance of the sinkhole attack was analyzed by using NS2 simulation software. Node 1 is chosen as the source node and node 20 is chosen as the sink node. The sink node is represented by red color. The hash value was calculated by using the RIPEMD algorhm which is stored in each sensor node.

When a node announces smaller path, we have to check whether that point is proper node malicious node.Sinkhole is identified by comparing the hash value which is stored in the database and the present value. The sinkhole node is represented by blue color. The simulation output of the detection of sink hole attack is shown in Fig. 11.4. The following parameters are used to evaluate the performance of network.

3. PACKET INTERCEPTION PROBABILITY:

The Packet interception probability is the probability of interception of shares. When the anomalous area becomes larger, the packet interception probability is more. In RIPEMD, the messages are transmitted via trusted paths, so the packet interception probability is very. The performance of the sinkhole attack was analyzed by using NS2 simulation software.

Node 1 as a source node and node 20 as a sink node. The sink node is represented by red color. The hash value was calculated by using RIPEMD algorithm which is stored in each sensor node. When a new node advertises to provide a shorter route to the base station, it is necessary to find if the new advertising node is a trustable node or a malicious node. The sinkhole node is identified by comparing the hash value which is stored in the database and the present value. The sinkhole node is represented by blue color. The simulation output of detection of sinkhole attack is shown in fig.11.4.

The performance of the sinkhole attack was analyzed by using NS2 simulation software. Node 1 as a source node and node 20 as a sink node. The sink node is represented by red color. The hash value was calculated by using RIPEMD algorithm which is stored in each sensor node. When a new node advertises to provide a shorter route to the base station, it is necessary to find if the new advertising node is a trustable node or a malicious node. The sinkhole node is identified by comparing the hash value which is stored in the database and the present value. The sinkhole node is represented by blue color. The simulation output of detection of sinkhole attack is shown in fig.11.4

A lot of students are coming towards Open Source Network Simulator as it is simple to use and free of cost. There are many open source simulators accessible these days, but because of its widespread appeal, the first thing that comes to mind when we discuss simulation is the NS2 simulation. To provide academics with comparative information about Open Source simulators, we have also concentrated on a few other useful simulators here. After becoming handy with simulators any one can use this simulator.

The proposed RIPEMD scheme acquires minimum packet interception probability which is observed and shown in Table 11.2

PACKET INTERCEPTION PROBABILITY

No of nodes		RIPED
50		0.002
100		0.004
150		0.006
200		0.010
250		0.013

4. NETWORK LIFETIME:

The network is the important metric in Wireless sensor network. The residual energy and energy consumed in each node determine the lifetime of the network. The network lifetime is defined at a time interval until the begining node or group of sensor nodes runs out of energy to send In RIPEMD, the probability of successful transmission is higher because the probability of intercepting packets by the adversary is less due to the transmission of data by trusted paths. It causes a reduction of number in the retransmissions of data and removes the burden of power consumption due to retransmission. A network lifetime of RIPEMD protocol is better compared to MD5.

TABLE 11.2 NETWORK LIFETIME

No of nodes	MD5	RIPEMD
30	200	850
50	500	980
100	640	1100
150	730	1190
200	870	1330
250	950	1400

4. PDR:~

The PDR is determined from the ratio of the number of successfully delivered packets reaches the destination are against and the packets are generated.The packet ratio is better

in RIPEMD differentiate to MD5. In RIPEMD, the probability of the message might be compromised is reduced due to trusted paths which are used to spread the information to the source node to the sink node. A selection about trusted node prevents node compromised attack and increases the chance of successful delivery of data to the sink node during its first transmission even increase of node density as well as compromised nodes.

TABLE 11.3 PACKET DELIVERY RATIO

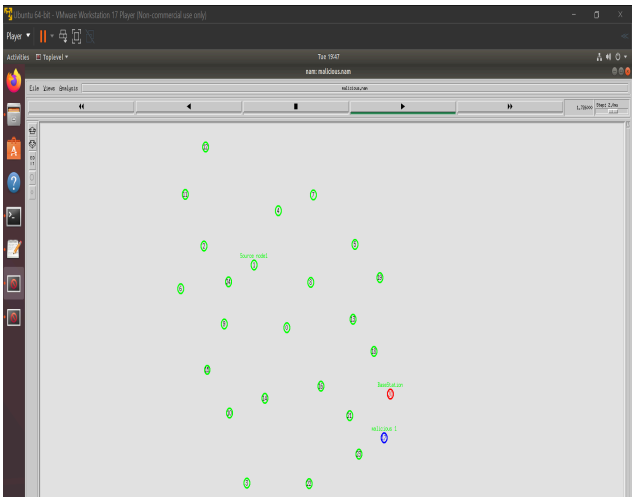
No of nodes	MD5	RIPEMD
30	92	95
50	93	96.2
100	91	94
150	86	92
200	84	91
250	83	90

5. FINAL-TO-FINAL DELAY:~

The data refers to the end time minus origination time of the data. When the number of compromised node increases, stable and sustainable state is retained because RIPEMD uses a trustable path and find the shortest multipath for transmitting data to reach the destination. RIPEMD reduces the End-to-End delay by up to 10%. It shows that RIPEMD has sustainable performance.

TABLE 11.4 FINAL-TO-FINAL DELAY

No of nodes	MD5	RIPEMD
30	64	56
50	76	62
100	98	76
150	155	98
200	178	114
250	187	123



a huge number of sensor nodes. Even though the network density is large, optimization in the delay is feasible because of trustable paths between sources and the sink nodes.

CONCLUSIONS

The mini-project using the AODV free looping routing protocol to detect and prevent black holes in networks of wireless sensors (WSNs). The main purpose was to enhance the safety and reliability of WSN by reducing the possible risk of entry attacks.We wanted to create a powerful and adaptable routing algorithm that could recognise abnormal behaviors characteristic of a black hole and conform to changing network conditions through the use of AODV. With the reason of detecting and avoiding illegally nodes from misbehaving with the network, the method consisted of integrating additional safety features within the AODV protocol.The project revealed that the resilience of the WSN against black hole attacks may be enhanced by utilizing the built-in capabilities of AODV and implementing security measures.

The proposed approach not only quickly discovered black holes but also minimized their effects by dynamically rerouting traffic via safe routes.Further, the inspection of the applied solution gave encouraging outcomes in terms of detection accuracy and effectiveness in prevention. An approach that showed sustainability and effectiveness, ensuring little network overhead and dependable communication.

REFERENCE

[1] Ruslan Dautov and Gill R Tsouri[2019] Effects of Passive Negative Correlation Attack on Sensors Utilizing Physical key Extraction in Indoor Wireless Body Area Networks.

[2] DAWEI LIU, MEMBER,YUEDONG XU, AND XIN HUANG[2017] Identification of Location Spoofing in Wireless Sensor Networks in Non-Line-of-Sight Conditions.

[3] OHIDA RUFAI AHUTU AND HOSAM EL-OCLA[2020] Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks.

[4]]LEI SHI, QINGCHEN LIU, JINLIANG SHAO, AND YUHUA CHENG[2020] Distributed Localization in Wireless Sensor Networks Under Denial-of-Service Attacks.

[5] OPEYEMI OSANAIYE, ATTAHIRU S. ALFA GERHARD P. HANCKE[2018] Denial of Service (DoS) Defence for Resource Availability in Wireless Sensor Networks.

[6] PATEL BHOOMIKA D,PATEL ASHISH D[2016] A Trust Based Solution for Detection of Network Layer Attacks in Sensor Networks.

[7] SHOUKAT ALI1, DR. MUAZZAM A KHAN, JAWAD AHMAD, ASAD W. MALIK, AND ANIS UR REHMAN[2018] Detection and Prevention of Black Hole Attacks in IOT & WSN.

[8] [8]SARITA AGRAWAL , MANIK LAL AND JAVIER LOPEZ[2017] Detection of Node Capture Attack in Wireless Sensor Networks .

[9] [9]WATEEN A. ALIADY AND SAAD A. AL- AHMADI[2019] Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Network.

[10] DHARA BUCH,D. C. JINWALA[2010] Denial of Service Attacks in Wireless Sensor Networks

[11] MANDEEP KUMAR AND JAHID ALI[2022] Taylor Sailfish Optimizer-Based Deep Stack Auto Encoder for Blackhole Attack Detection in Wireless Sensor Network MISS. PRACHI S. MOON MR. PIYUSH K. INGOLE[2015] An Overview on: Intrusion Detection System with Secure Hybrid Mechanism in Wireless Sensor Network.

[12] ASHISH JAIN MADHU SHARMA[2016] Wormhole Attack in Mobile Ad-hoc Networks.

[13] Abdulmalik Danmallam Bello, Dr. O. S. Lamba, 2020, How to Detect andMitigate Sinkhole Attack in Wireless Sensor Network International Journalof Engineering Research & Technology (IJERT) Volume 09, Issue 05 Semagn Shifere et al. Department of Computer Science Woldia University, Ethiopia ,Volume 6, Issue 2, February – 2021 International Journal of Innovative Science and Research Technology ISSN No:-2456-2165.

[14] Sihem Aissaoui & Sofiane Boukli, Sinkhole attack detection based on SVM in wireless sensor network, international journal of wireless networks and broadcast technologies,IGI Global, vol. 10(2), pages 16-31, July.

[15] Neha Singh, Kamakshi Rautela [2016], International Journal of Engineering and Computer Science ISSN: 2319 – 7242, Volume 5, pp. no. 17544-17548.

[16] Dhivya M et al. vol.2, 2021, Detection and Prevention of Sinkhole Attack inWireless Sensor Network using Armstrong 16-digit Key Identity and GANNetwork.

[17] Sumit Pundir et al. [2020] designed efficient sinkhole attack detectionmechanism in egde based IoT deployment 2017, pp. 359–365, doi: 10.1109/CESYS.2017.8321299.

[18] K. Karthigadevi and M. Venkatesulu, "Based on Neighbor Density Estimation Technique to Improve the Quality of Service and to detect and Prevent the Sinkhole Attack in Wireless Sensor Network," 2019 IEEE International Conference on Intelligent Techniques in the control, Optimization and Signal Processing (INCOS), Tamilnadu, India, 2019, pp. 1–4. 16.

[19] Vidhya, S, "Sinkhole Attack Detection in WSN using Pure MD5 Algorithm." Indian Journal of Science and Technology 10.24 (2017).