International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209995 Volume 8, Issue 5, September – October (2021)

RESEARCH ARTICLE

A Novel Technique for Blackhole Discernment Employing Big Data Analytics in IoT Networks

Gauri Mathur
School of Computer Science and Engineering, RIMT University, Mandi Gobindgarh, Punjab, India
gauri.mathur@lpu.co.in

Wiqas Ghai
School of Computer Science and Engineering, RIMT University, Mandi Gobindgarh, Punjab, India
ghaialpha@gmail.com

Received: 08 September 2021 / Revised: 13 October 2021 / Accepted: 17 October 2021 / Published: 27 October 2021

Abstract – Internet of Things is connection of equipment, machine, software and everything around us to make smart things which have unique IP address to distinguish from other things. In Internet of Things everyday objects have capabilities to identify, sense and process the data so they can communicate with each other generating huge volumes of data. But data security is the major issue as when communication takes place the data can be altered through malicious attacks taking place on network while the data is being transmitted from different devices. So, in this paper a novel totalitarian approach is proposed for detection of blackhole attack which drops the packets being transmitted in the network leading to hacking and loss of data. So, in order to eliminate this DoS attack from the network proposed technique can be used where occurrence of malicious infected path results in initiation of request sent by any local node to all of its neighbor's node for verifying the presence of the malicious path in their routing tables which has a high percentage of usage. We have used the approach of a modified routing table along with analysis of the threshold value generated by nodes which generates huge volume of big data and variation in amount of data generated by malicious nodes we can identify suspicious links before the attack is initiated and starts disturbing within the network. This is done to establish legitimacy of the node and on the corroboration of a malicious attack a blacklisting message is broadcasted to exclude the colluder nodes from the network. Results and analysis of this technique is been done on the basis of packet delivery ratio, throughput, power consumption and congestion control. Along with this comparative analysis of this technique is done with the other existing techniques proposed by various renowned researchers for identifying these blackhole attacks taking place in IoT Networks. The proposed technique makes use of a modified routing table and utilizes Big Data analytics to accurately ascertain the blackhole nodes in the IoT network. The detection and isolation of colluder nodes is being done accurately with minimalistic consumption of resources as opposed to some of the existing techniques, which may require high power consumption, synchronization, as well as other resources thereby making these techniques resource intensive. Since this technique makes use of multivariate parameter, it is more resilient to faults. Our approach also aims to alleviate the security and privacy concerns associated with big data thereby being a potential flag winner for the organizations.

Index Terms – Blackhole Attack, Internet of Things, Big Data, Malicious Node, Cooja Simulator, Big Data Analytics.

1. INTRODUCTION

Internet of Things is connection of equipment, machine, software and everything around us to make these as smart things, which have unique IP address to distinguish from other things. Smart home, wearable, health care, smart environment are some examples of IoT applications. In paper [1] Internet of Things connects devices where everyday objects can be given capabilities of identifying, sensing, networking and processing capabilities so they can communicate with each other and transfer large amount of data.

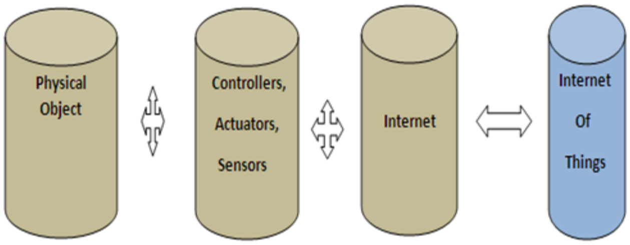


Figure 1 Communication of IoT Devices

As shown in Figure 1 these physical devices consist of powerful sensors, have capability to communicate anywhere, anytime, with any internet connection, and can be used for any business purpose. The major advantage of using IoT is that it does not require any central governing authority and does not require huge infrastructure support. The popularity of IoT devices discussed in paper [2] brings with it a plethora of problems with some noteworthy malware targeting IoT devices only. To be more particular, Internet of Things provides the creation of mixture of privacy risks to customer and the type of personal and sensitive information, which can be collected from consumer. Smart home services industries, medical devices are more prone to cyber-attack as mostly service provider never bother about security constraints in the starting. The major security threats in a smart home and medical fields as stated by researchers in [3] are (DDoS) attacks and hacking of data, confidentiality issues, unauthorized access etc.

Some of the security threats in the IoT network are as follows:

a) End to End Data life cycle protection: Security of information in Internet of Things environment as proposed in [4] is required to provide end to end protection of information throughout the network. This data is gathered from various devices that are connected to each other and instantly shared with other devices. Many hackers and intruders perform malicious and DoS attacks while the data is transmitted through IoT devices to alter or hijack the data.

b) Secured planning: As stated by researchers in [5] different devices should be capable of managing high security level as communication between various IoT devices may vary. For instance, when local sensors are used in the home based network they should work on same security policy when communicating with external devices

c) Issues in Smart Home security and medical area: Smart home services are more prone to cyber- attack as mostly service provider never bothers about security constraints in the starting. The major security threats in a smart home and medical fields as stated by researchers in [6,7] are (DDoS) attacks and hacking of data, confidentiality issues, unauthorized access etc.

d) Authenticity of Data**:** The information being transmitted should be authenticated. One should follow an authentication process which allows transmission of data from only authentic devices.

1.1. Usage of Big Data in IoT

Recent studies done by authors in [8, 29] claim that the number of devices connected to the Internet has surpassed the number of human beings in the world. All of this coupled by IoT network gives rise to insurmountable amounts of information as depicted in Figure 2. The overlap between the growth of data consumption by IoT devices and the number of devices connected to the IoT network signals the exponential rise of Big Data. Furthermore, the data generated by the mesh of IoT devices bearing temporal and spatial characteristics by its sheer volume is classified as Big Data and it is at a serious threat of being maligned and misused. Big data is of prime significance and needs to be secured as often it bears confidential information which is paramount to the organization’s survival. An organization should strive to provide security and establish trust as sensitive data could very well turn out to be a potential goldmine to the prospective attackers. Communication among devices leads to a flood of unstructured, semi-structured and structured data and this is the root cause of a profusion of security breaches. The gamut of precious information presents a potential gold mine to the attackers of an IoT network and hence presents a big security threat. This aggressive growth stated in [9] has led to new challenges in data collection efficiency, security and data analysis. A secure solution for sensitive information comprising of big data is of utmost importance as its proper implementation can fuel any big data initiative. Authors in [10] said that one of the grave threats to the security and integrity of Big Data is a Distributed Denial of Service (DDoS) attack [30] which works by disrupting the services of a network machine or host by making the network resource inaccessible to the intended users.

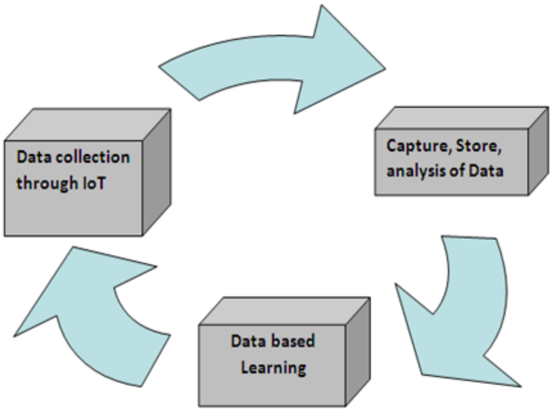


Figure 2 Big Data in IoT

1.2. Blackhole Attack in IoT Networks

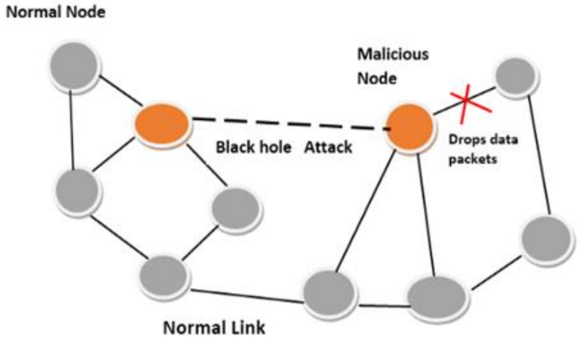


Figure 3 Blackhole Attack on IoT

As depicted in Figure 3 the blackhole attack [21,23] is a DoS attack where in a colluder node advertises a fraudulent path to the destination. This colluder node acts as a sink absorbing all incoming packets with the intention of dropping the same. In the network where all IoT devices devices are communicating with each other, each node is dependent on the other node for forwarding of data and the intruders uses this dependency for inserting the colluder nodes within the network. So, the malicious nodes start dropping packets and hence the blackhole attack takes place. The network of IoT devices[25,28] is constrained in terms of computation and power.

In this study, we aim to alleviate the privacy and security threats prevalent in an IoT network by accurately identifying and isolating the nodes which are a part of the blackhole attack. The problem statement is therefore the guaranteed isolation of participating nodes in the blackhole attack thereby preventing the loss of data. The guarantee stems from the fact that the vast amount of data generated by the devices in the IoT network has been used for decision making and at the same time the authenticity, integrity and security of the IoT network has been maintained. Thus, our technique has the key objectives of accurately detecting the blackhole nodes, isolating them, simulating the process on the Cooja simulator, collection and analysis of results using Google's Big Query analytics platform as well as comparison of our technique with existing techniques of blackhole detection. The prime motivation behind the study is to provide a secure, reliable as well as resilient system which is able to thwart blackhole attacks so that the IoT network can operate without any challenges thereby extending their utility in military, financial sectors, defense as well as medical fields.

This paper proceeds as follows. Section 2 introduces blackhole attack and its existing techniques. Section 3 describes methodology of detection of blackhole attack and its isolation from IoT Network. Section 4 shows the results of implementation of this technique on basis of throughput, packet delivery Ratio, congestion control and power consumption. Also, performance of proposed technique is compared with other existing techniques. Finally, Section 5 describes conclusion and future work.

2. RELATED WORK

Paper [11] mentions baiting technique which depend on its own node id and identification of blackhole node is initiated through broadcast of a bait request to all of its nearby nodes. The bait request consists of source Wireless Communications and Mobile Computing id and source sequence number (SSN) if the source node receives reply then the node verifies when there is a reply which has larger DSN value than its own SSN which informs that the reply came from a black-hole as no node within the network have a larger DSN than SSN of the source node. Once blackhole node is identified the source node will broadcast a blackhole detection alarm to its neighbors.

The researchers in [12] have proposed a technique which incorporates Cooperative Bait Detection Method Scheme. In CBDS three phases of detecting Black hole are implemented as Bait, Reverse Trace and Reactive Defense. In first phase source node chose any one of the neighbors to transmit a bait request via its own id. In second phase various suspicious nodes list is initiated from the RREP of the bait RREQ, along with which the neighbor nodes enter in active mode in order to detect whether an attacker node is existing in the path or not. A black-hole alarm is broadcasted to neighbor nodes for each blackhole detected in the network. In third phase the source node will compare the PDR with pre-determined threshold value if it is lesser than a predetermined threshold value then it executes the first phase again.

Authors in paper [13] discussed a technique which depends on usage of fake id scheme. The source node propagates a broadcasting request which consists of an id that is not existing within network. Then only black hole node will reply to that RREQ as it normal can reply to any RREQ which claims that it has the best path in the network. So, when a blackhole node is detected an alert message is broadcasted throughout the network. And the source node keeps a track if there is any reduction below a threshold value, then it initiates re-broadcasting of the message.

In [14], the authors proposed a model which initiates flooding of fake requests in the network. Any node replying to fake messages can be considered as a suspicious node because the suspicious node starts forwarding packets to the destination node then that means that blackhole node is present within the network. The proposed model has a localization system which can identify the position and presence of the black hole node.

In [15], the author has proposed a new system which is dependent on a particular kind of nodes which is known as guard nodes that helps in identifying the suspicious nodes in the network which perform the blackhole attack. They are nodes which are added in silent mode which keep a check on behavior of rest of the nodes within IoT network. Also in order to record the behavior of other nodes added in network they keep track of updated tables.

In [16], authors have proposed a model which uses concept of validity bit which is attached in RREP and the attacker node is not aware of validity bit that shall be transmitted while transmitting the RREP to other nodes. Later, validity bit is checked by the sender if it is set to one, the node will use the proposed path for data transmission otherwise it checks the RREP given from the malicious node and then discards it.

In [17] the researchers have made a model known as SAODV which identifies blackhole by trusting the opinion of neighbor nodes. Every node in SAODV maintain two tables one is list of neighbors where it stores id's of a neighbor nodes and the other is opinion list used to identify activity performed by the nodes within the network. Once the source node broadcasts the opinion message to neighbors if it receives a reply for route request and it request the opinions of its neighbors regarding the node claiming that they have the shortest path.

Authors in [18,19] have proposed a model which uses fabricated request in order to identify the black-hole nodes in the network. A source node will broadcast fabricated request to other nodes within the network and if blackhole node response to the fake request then it will be considered as malicious node node. Average value of DSN is stored by source node which is compared with reply DSN numbers and if it is closed to average value then the node is listed a blackhole node else it is considered as normal node. It also uses trust value and digital signatures technique and is one of the most promising technique for detecting the black hole attack.

In paper [22,26,27] hierarchal trust based scheme has been proposed for Smart Grid stations where the Network is categorized into three segments and from each segment one cluster head is selected using cluster head selection algorithm. The cluster head will collect the data and transfer to the Sink. Hierarchical trust evaluation model implemented to differentiate good nodes from bad ones where cluster head has responsibility for managing the history of dropped packets.

The proposed technique consumes less power as compared to some of the already existing techniques. It has also shown outstanding performance in terms of ease of implementation, fault tolerance, synchronization as well as quality of service in comparison to some of the already existing techniques. The proposed technique also has the distinction of using Big Data analytics for the purpose of detecting the blackhole nodes with certainty. The multivariate parameter approach adopted by the proposed technique ensures that the blackhole nodes are detected with certainty and are isolated from the rest of the network thereby mitigating the security risks posed by them in the network. The proposed technique is also free from the drawbacks of approaches which rely on a central singular authority whose failure may compromise the security and integrity of the entire network.

3. PROPOSED METHODOLOGY

The proposed technique looks to modify the routing table which forms the basis of routing packets. A clever use of Big Data analytics also ensures that we are able to reliably detect and finally isolate the colluder nodes. The successful isolation and removal of colluder nodes from the IoT network ensures that the participating nodes can carry out communication without any hurdles and the entire communication can proceed in a safe and secure manner. A colluder/malicious node in an IoT network [24,25] has the potential to seriously hamper the functioning of an IoT network. An attacker may gain control of a node thereby transforming it into a malicious node and may drop some of the packets, alter them in some way as well as gain control of the information being passed on the network. In order to fully comprehend the extent of this problem, let us consider a sample scenario in which there are 25 nodes in the network. All these 25 nodes are connected to each other and the initial state of the network is depicted in Figure 4 the routing information is also present in the adjoining routing Table 1 which contains information about destination, path as well as information about the number of hops. The information in the routing table can be further analyzed if we consider the task of reaching node 25 from node 3. The path being taken is given in the routing table as 3->8->22->19->18 where 25 acts as the destination node and the number of hops are 6. A clever use of the information present in this routing table forms the basis of our novel approach. The nodes Cs and Cd are overtaken by malicious attackers and are acting as colluder nodes in the routing table for the network with the advent of the potential colluder nodes is present in Table 1 and signifies the updated and changed path along with updated hop information. A pattern of high usage among the nodes labelled as Cs and Cd is observed and the other striking feature which indicates the colluder node presence is the drop in the number of hops. The following steps, when morphed and simulated on nodes with the help of Cooja simulator, help us in detecting the blackhole nodes.

i) Firstly, a local node will send information regarding suspicious nodes to all the nodes connected in the network and if the neighbor nodes also have high usage of these suspected nodes then other nodes will be intimated.

ii) The information about the amount of Big data generated by these nodes at alternating time intervals is broadcasted to neighbor nodes along with routing information.

iii) After getting a confirmation reply from the neighbor node, the initiator node broadcasts an encrypted message containing timestamp/flag which can only be decrypted by legal and legitimate nodes. A node whose signature is present in an encrypted message is considered a legitimate node. Missing node signatures can be indicative of blackhole presence.

iv) Apart from this, the variation of generated parameters from predetermined threshold values generated by these malicious nodes which are transmitting huge volumes of Big data is the key indicator for identification of malicious paths and their activity.

v) Once the malicious nodes are confirmed, the initiator node will send a broadcasting message to blacklist the nodes from the network. The above steps include usage of routing tables along with Big data analytics for detecting the blackhole attack in the network and isolating the illegal nodes.

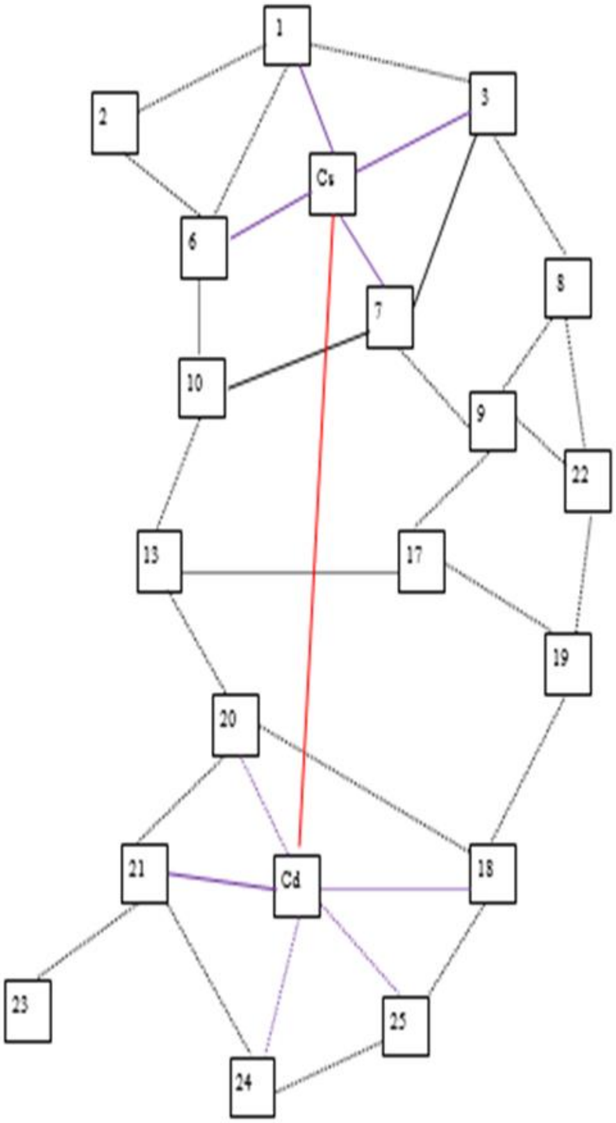


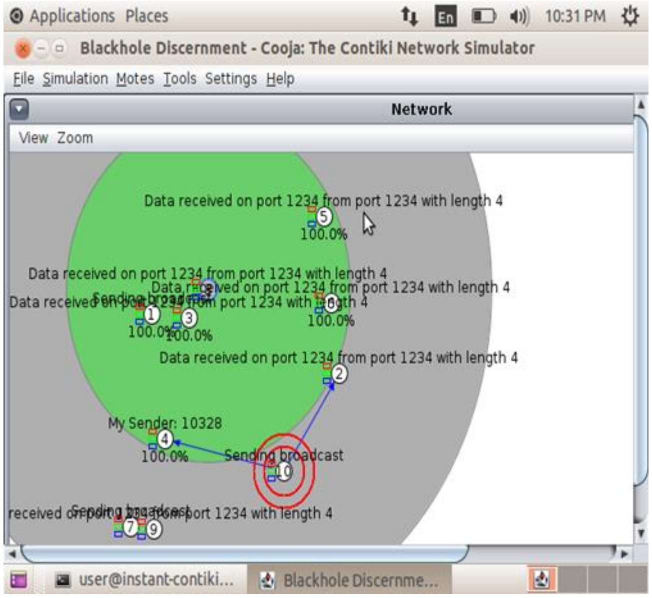
Figure 4 Advent of Blackhole Attack Being Followed by Malicious Node

Blackhole Present		
Destination	Path	Hops
1	–	0
2	2	1
3	3	1
7	6	2
8	3	2
9	3->7	3
10	6	2
13	6	3
17	7>3>9	3
18	Cs>Cd	3
19	3>8>22	4
20	Cs>Cd	3
21	Cs>Cd	3
22	3>8	3
23	Cs>Cd>21	4
24	Cs>Cd	3
25	Cs>Cd	3

Table 1 Routing Table with Advent of Blackhole Attack

Big Data analytics is useful in pointing us in the right direction and helps us in identifying and isolating the colluder node. In Figure 5 a network of 1000 nodes is created using the Cooja simulator [20] which helps in simulating the motes. It allows very close inspection of minute details of the network behavior and how the system can be set up and testing can also be performed using this flexible simulator.

In Algorithm 1 logs file is generated and Packet Delivery Ratio Threshold, Mote Throughput Threshold and Power Consumed Threshold are generated. Further in Algorithm 2 Packet Delivery Ratio Threshold, Mote throughput Threshold and Power Consumed Threshold is received as input to mark the suspected nodes as colluder nodes.


Applications Places
10:31 PM
Blackhole Discernment - Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
Network
View Zoom
user@instant-contiki...
Blackhole Discernme...

Data received on port 1234 from port 1234 with length 4

Data received on port 1234 from port 1234 with length 4

Data received on port 1234 from port 1234 with length 4

Sending broadcast

Data received on port 1234 from port 1234 with length 4

My Sender: 10328

Sending broadcast

received on port 1234 from port 1234 with length 4

Sending broadcast

Figure 5 Mote Isolation Using Cooja Simulator

Input :

Generated logs of information

Output:

Pdrthresh : Packet Delivery Ratio Threshold

Mthresh : Mote Throughput Threshold

Pconsumedthresh : Power Consumed Threshold

```
totalPackets  = total packets received
totalTime = total time taken
Mtput = Mote Throughput
pdr = Packet Delivery Ratio
totalSent = total packets sent
totalUnits = total Power Consumption
foreach record in Logs do
    if Logs[i].packetsRecevied != 0 then
        totalPackets = totalPackets + Logs[i].packetsReceived
        totalTime = totalTime + Logs[i].totalTime
    i = (1… n)
Mtput = totalPackets / totalTime
Mthresh = Mtput / n
totalPackets = 0
foreach record in Logs do
    if Logs[i].packetsReceived != 0 then
        totalPackets = totalPackets + Logs[i].packetsReceived
        totalSent = totalSent + Logs[i].packetsSent
pdr = totalPackets / totalSent
Pdrthresh = pdr / n
foreach record in Logs do
    totalUnits = totalUnits + Logs[i].unitsConsumed
Pconsumedthresh = totalUnits / n
```

Algorithm 1 DetectColluderNodes (Logs, Pdrthresh, Mthresh, Pconsumedthresh)

Input :

Records : Log of data generated by motes

Pdrthresh : Packet Delivery Threshold

Mthresh : Mote Throughput Threshold

Pconsumedthresh : Power Consumed Threshold

Output :

MarkNodes : Mark Nodes to hold information about colluder nodes

```
throughPut =  Throughput
pdr = Packet Delivery Ratio
Pconsumed = Power Consumed
foreach log in Records do
    if Records[i].packetsReceived != 0 then
        throughPut = Records[i].packetsReceived / Records[i].totalTime
        pdr = Records[i].packetsReceived / Records[i].packetsSent
    if Records[i].unitsConsumed != 0 then
        Pconsumed = Records[i].unitsConsumed
    if throughPut > Mthresh and pdr > Pdrthresh  and Pconsumed > Pconsumedthresh  then
        MarkNode[i] = true
    i = 1…n
```

Algorithm 2 MarkColluderNodes (Records, Pdrthresh, Mthresh, Pconsumedthresh, MarkNodes)

The data generated by the devices in the IoT network can easily run into volumes and if properly analyzed can give rise to a gamut of useful information that can be utilized in a myriad of ways to obtain meaningful results. The data generated by the motes in our simulated IoT network on the

Cooja simulator is converted into a CSV format for data ingestion in Google Cloud Platform’s Big Query.The sample set contains the data generated by 1000 motes in the Cooja simulator. The Big Data tool by Google Cloud platform namely Big Query helps us analyze the information given by the IoT network. The information is loaded in the form of a dataset fed to BigQuery and the CSV information is then loaded in the form of a table.Post the configuration of BigQuery. The SQL workspace by Big Query is being utilized and appropriate queries are used to setup subsets of data hich is being brought about by various factors namely throughput, packet delivery ratio, power consumption. The process of isolating the malicious nodes is depicted using level 2 data flow diagram in Figure 6. The efficiency and efficacy of the network brought about by these factors and subsequent plotting of the same will point us in the direction to identify reliably and with certainty colluder nodes.

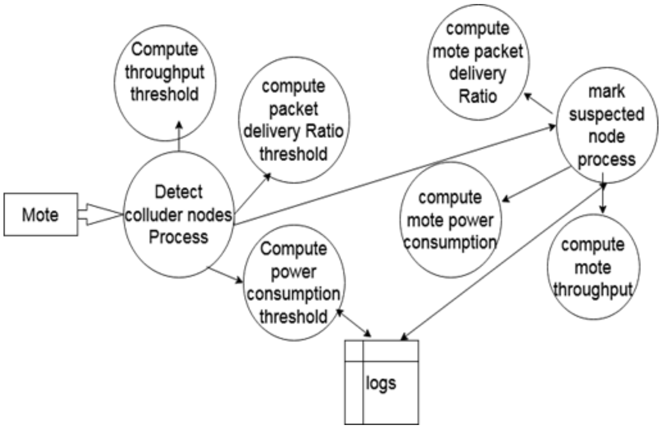

Compute throughput threshold
compute packet delivery Ratio threshold
compute mote packet delivery Ratio
mark suspected node process
Mote
Detect colluder nodes Process
compute mote power consumption
Compute power consumption threshold
compute mote throughput
logs

Figure 6 DFD for Isolation of Blackhole Nodes in IoT Network

4. RESULTS AND DISCUSSIONS

4.1. Throughput

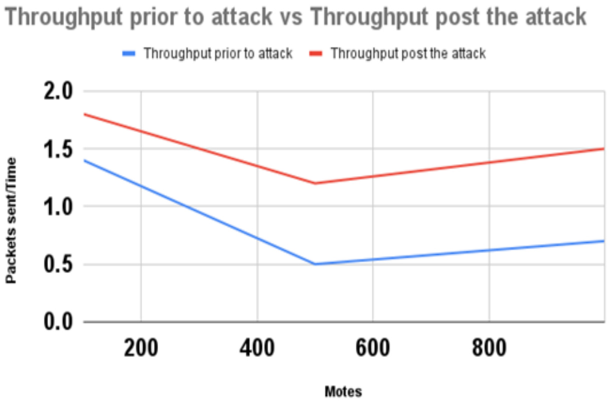


Figure 7 Throughput Comparative Data Plot of Pre vs Post Colluder Node Infusion

The quantity of data packets received by the receiver per unit of time is known as throughput and is measured in bits per second.

Throughput = Σ NP/Σ TT (1)

The above formula has been used to compute the throughput of the network pre and post the influx of the colluder nodes in the network where NP = Total Number of Packets and TT= Total Time. Above formula has been used to compute the throughput of the network pre and post the influx of the colluder nodes in the network.

The Figure 7 showcases the variation of throughput on the advent of the colluder nodes. This points us in the direction of identifying the colluder nodes. The nodes with high usage are the ones which are potential colluder nodes as the high usage raises a strong suspicion.

4.2. Packet Delivery Ratio

It is a strong indicator of the network performance in which we are able to determine how well the network is performing or in short the efficiency and efficacy of the network. In Figure 8 the packet delivery ratio can be measured as the ratio of the total number of packets delivered vs the lost packets on the network. It can be clearly seen that in the data set, the Packet Delivery ratio of some of the nodes have clearly risen as compared to the ratio prior to the advent of the colluder nodes. This is one of the key indicators of the presence of colluder nodes infiltrating and potentially harming the network.

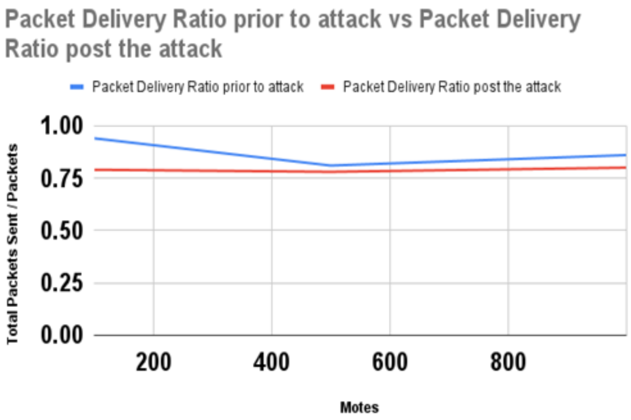


Figure 8 Graph Plot of Packet Delivery Ratio of Pre and Post Colluder Node Infiltration

4.3. Power Consumption

Power Consumption of Nodes in the IoT network varies with usage. If a node is consuming and emanating more data, then this should push its power consumption. As shown in Figure 9 if a node is frequently using more power as opposed to its normal usage then coupled with other factors it's an indication that some malicious nodes are present inside the network. The visualization of Power Consumption of nodes in the pre and post the advent of malicious nodes is done with the help of Data Studio and is as follows:

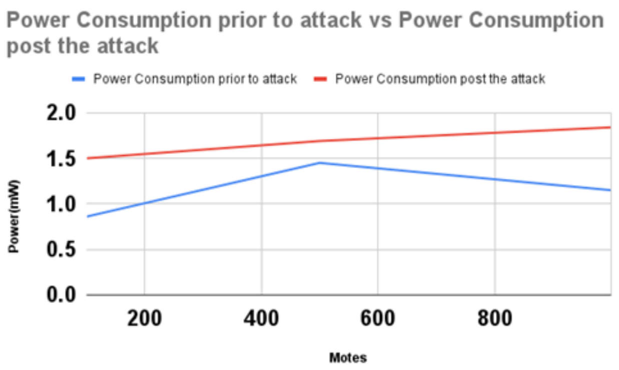


Figure 9 A Comparative Graph Plot of Power Consumption in IoT Network in Data Studio Prior to and Post the Advent of Colluder Nodes

4.4. Congestion Factor

The rise in the number of connected devices also leads to the congestion of the network. The major objective of the IoT network is to deploy highly effective and high quality services, which enables the network to deliver smart services. The congestion factor of nodes shown in Figure 10 in the IoT network is an indicator of the node capacity wherein it can be used to check for nodes exhibiting a high degree of congestion.

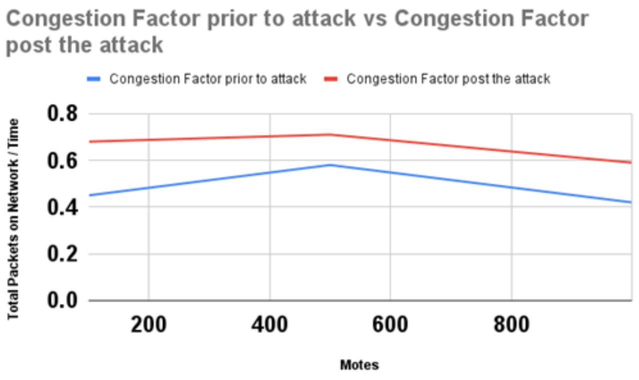


Figure 10 A Comparative Graph Plot of Congestion Factor in IoT Network in Data Studio Prior to and Post the Advent of Colluder Nodes

4.5. Comparative Analysis of Our Novel Technique with Existing Techniques

This approach requires less power consumption as compared to existing techniques. This technique has shown outstanding results related to ease of implementation, synchronization, fault tolerance and quality of service as compared to the already existing approaches discussed in Table 2. Moreover, this is the only approach using big data analytics for identification of blackhole attack. The proposed totalitarian technique for detecting Blackhole attack outperforms some of the other techniques for Blackhole detection such as Baiting technique, Cooperative baiting technique and SAODV as these techniques are solely based on keeping track of routing table or calculating threshold values which may lead to suboptimal detection of colluder nodes. The proposed technique takes into account multiple parameters which makes it more accurate and resilient.

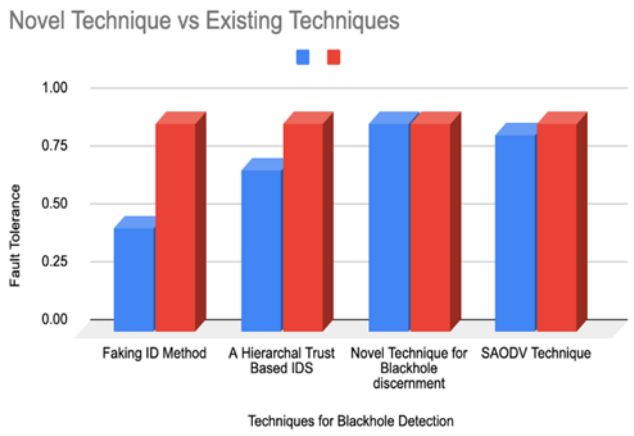


Figure 11 Analysis of Fault Tolerance with Existing Techniques

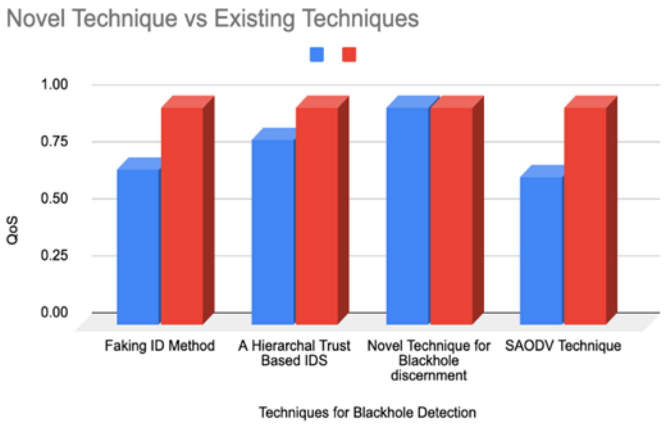


Figure 12 Analysis of QoS with Existing Techniques

Graphs depicted in Figure11 and Figure 12 shows that proposed technique outshines some of the existing techniques of blackhole detection like SAODV, Hierarchical Trust based IDS, and faking id technique in terms of QoS and Fault tolerance. The trust based technique involves maintaining clusters which are managed by a head node and it is the sole responsibility of the head node to ensure the detection of Blackhole nodes in the network. The cluster head technique also requires heavy synchronization among nodes as opposed to the proposed technique. The proposed technique once again outperforms the trust based technique as it takes a decision based on multiple parameters and unlike cluster head technique is not dependent on a single node whose failure may lead to a compromised network. The flooding fake IDs technique is limited to flooding of fake messages, which may not be responded to by malicious nodes, which has a serious limitation of maintaining Quality of Service.

METHODOLOGY USED	**FAULT TOLERANCE**	**SYNCHRONIZATION**	**RESOURCES NEEDED**	**QOS**
Baiting Technique	High	Synchronization is required	Less resources are Required	Low Delay
Cooperative Bait	High	Synchronization is needed.	Less resources are Required	Low Delay
SAODV Technique	High	No synchronization is required.	Medium as neighbor data is needed	Moderate delay
Novel technique for Detection of Blackhole Discernment	High	No synchronization is required.	Minimal resources are required as routing table undergoes modification	No Delay
Faking id Method	Low	Synchronization is needed	Medium as neighbor data is needed	Moderate Delay
A Hierarchal Trust Based IDS	Moderate	Synchronization is needed	Medium as neighbor data is needed	Low Delay

Table 2 Comparative Analysis of Our Proposed Technique with Existing Techniques

5. CONCLUSION AND FUTURE WORK

The approach discussed above is highly cost effective and is easy to implement, as it does not need any infrastructure. No synchronization is required for implementing this technique. This approach is completely authentic and will leave no stone unturned to detect the malicious nodes and isolating them from the network.

In future, a thorough analysis can be carried out in order to analyse the adoptability of this approach with changing factors. Also, the technique can be further optimized in terms of performance metrics to ensure that the detection is done as soon as the colluder nodes start presenting themselves in the network. The algorithmic technique can be highly useful in the prevention of botnets which are a real threat to the network security and can pose a significant threat to the security and integrity of the network. The potential of the technique can be further explored in terms of its detection capability when it comes to the detection, prevention and elimination of further threats to the security of the network. The potential of the technique can be further explored in terms of its detection capability when it comes to the detection, prevention and elimination of further threats to the security of the network. The proposed algorithmic technique has displayed its efficacy however, a detailed analysis and study of the proposed algorithmic technique is required to be carried out in order to determine its feasibility and its acute potency.

REFERENCES

[1] Hameed, Sufian, Faraz Idris Khan, and Bilal Hameed. "Understanding security requirements and challenges in Internet of Things (IoT): A review." Journal of Computer Networks and Communications 2019 (2019).

[2] Yaqoob, Ibrar, Ejaz Ahmed, Ibrahim Abaker Targio Hashem, Abdelmuttlib Ibrahim Abdalla Ahmed, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. "Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges." IEEE wireless communications 24, no. 3 (2017): 10-16.

[3] Bhavadharini, R. M., S. Karthik, N. Karthikeyan, and Anand Paul "Wireless networking performance in IoT using adaptive contention

window." Wireless Communications and Mobile Computing 2018 (2018).

[4] M. Mahmud Hossain, M.Fotouhi, and R. Hasan, “Towards an Analysis of Security Issues, Challenges and Open Problems in the Internet of Things,” in Services (SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp.21-28

[5] Sharma, Neha, Usha Batra, and Sherin Zafar. "A neoteric swarm intelligence stationed IOT–IWD algorithm for revolutionizing pharmaceutical industry leading to digital health." In Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach, pp. 1-19. Academic Press, 2020

[6] Li, L. Da Xu, and S. Zhao, “The Internet of Things: A Survey,” in [Information Systems Frontiers], ©[Springer]. doi: [10.1007/s10796-014-9492-7], New York, 2014, pp.243-299.

[7] Bhavadharini, R. M., S. Karthik, N. Karthikeyan, and Anand Paul. "Wireless networking performance in IoT using adaptive contention window." Wireless Communications and Mobile Computing 2018 (2018).

[8] Bashir, Muhammad Rizwan, and Asif Qumer Gill. "Towards an IoT big data analytics framework: smart buildings systems." In 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), pp. 1325-1332. IEEE, 2016.

[9] Lee, Carman KM, C. L. Yeung, and M. N. Cheng. "Research on IoT based cyber physical system for industrial big data analytics." In 2015 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), pp. 1855-1859. IEEE, 2015.

[10] Lee, Jay, Hossein Davari Ardakani, Shanhu Yang, and Behrad Bagheri. "Industrial big data analytics and cyber- physical systems for future maintenance & service innovation." Procedia Cirp 38 (2015): 3-7

[11] Yasin, Adwan, and Mahmoud Abu Zant. "Detecting and isolating black-hole attacks in MANET using timer based baited technique." Wireless Communications and Mobile Computing 2018 (2018).

[12] Dumne, P.R. and Manjaramkar, A., 2016, September. Cooperative bait detection scheme to prevent collaborative blackhole or grayhole attacks by malicious nodes in MANETs. In 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 486-490). IEEE.

[13] P.-C. Tsou, J.-M. Chang, Y.-H. Lin, H.-C. Chao, and J.-L. Chen, “Developing a BDSR scheme to avoid black hole attack based on proactive and reactive architecture in MANETs,” in Proceedings of the 13th International Conference on Advanced Communication Technology: Smart Service Innovation through Mobile Interactivity, ICACT 2011, pp. 755–760, Seoul, Republic of Korea, February 2011.

[14] B. Singh, D. Srikanth, and C. R. S. Kumar, “Mitigating effects of black hole attack in mobile Ad-Hoc NETworks: Military perspective,” in Proceedings of the 2nd IEEE International Conference on Engineering and Technology, ICETECH 2016, pp. 810–814, Coimbatore, India, March 2016.

[15] A. R. Rajeswari, K. Kulothungan, and A. Kannan, “GNB-AODV: guard node based –aodv to mitigate black hole attack in MANET,” International Journal of Scientific Research in Science, Engineering and Technology, vol. 2, no. 6, pp. 671–677, 2016.

[16] S. R. Deshmukh, P. N. Chatur, and N. B. Bhople, “AODV-Based secure routing against blackhole attack in MANET,” in Proceedings of the 1st IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016, pp. 1960–1964, Bangalore, India, May 2016.

[17] S. Dhende, S. Musale, S. Shirbahadurkar, and A. Najan, “SAODV: Black hole and gray hole attack detection protocol in MANETs,” in Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 2391–2394, Chennai, India, March 2017.

[18] M. Sathish, K. Arumugam, S. N. Pari, and V. S. Harikrishnan, “Detection of single and collaborative black hole attack in MANET,” in Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016, pp. 2040–2044, Chennai, India, March 2016.

[19] Ali, Shoukat, et al. "Detection and prevention of Black Hole Attacks in IOT & WSN." 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC). IEEE, 2018.

[20] Weingartner, Elias, Hendrik Vom Lehn, and Klaus Wehrle. "A performance comparison of recent network simulators." In 2009 IEEE International Conference on Communications, pp. 1-5. IEEE, 2009

[21] Guptha, Y.P.K. and Madhu, M., 2017. Improving security and detecting black hole attack in wireless sensor network. International Journal of Professional Engineering Studies, 8(5), pp.260-265.

[22] Otoum, S., Kantarci, B. and Mouftah, H.T., 2017, May. Hierarchical trust-based black-hole detection in WSN-based smart grid monitoring. In 2017 IEEE international conference on communications (ICC) (pp. 1-6). IEEE.

[23] Chhabra, A., Vashishth, V. and Sharma, D.K., 2017, March. A game theory based secure model against black hole attacks in opportunistic networks. In 2017 51st Annual conference on information sciences and systems (CISS) (pp. 1-6). IEEE.

[24] P. Hemalatha, J. Vijithaananthi, “An Effective Performance For Denial Of Service Attack (DoS) Detection” IEEE, International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)”, pp 229 – 233, Palladam, India, 10 – 11 February 2017.

[25] Abdullah Aljumah, Tariq Ahamed Ahanger, “Futuristic Method to Detect and Prevent Black-Hole Attack in Wireless Sensor Networks” IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.2, 05 February 2017.

[26] Saurabh Sharma, Dr. Sapna Gambhir, “CRCMD&R: Cluster and Reputation based Cooperative Malicious Node Detection & Removal Scheme in MANETs”, IEEE, 11th International Conference on Intelligent Systems and Control (ISCO), pp 36 – 340, Coimbatore,India, 5-6 January 2017.

[27] Mert Melih Ozcelik, Erdal Irmak, Suat Ozdemir “A Hybrid Trust Based IDS for WSN” IEEE, Networks, Computers andCommunications (ISNCC), pp 1 – 6, Marrakech, Morocco, 16-18 May 2017

[28] Gurjinder Kaur1, V.K. Jain, Yogesh Chaba “Detection and Prevention of Black hole Attacks in WSN” Springer, International Conference on Intelligent, Secure, Dependable Systems in Distributed and Cloud Environments (ISDDC), pp 118-126, Vancouver, BC, Canada, 25-27October 2017.

[29] Marjani, Mohsen, Fariza Nasaruddin, Abdullah Gani, Ahmad Karim, Ibrahim Abaker Targio Hashem, Aisha Siddiqa, and Ibrar Yaqoob. "Big IoT data analytics: architecture, opportunities, and open research challenges." ieee access 5 (2017): 5247-5261.

[30] Hameed, Sufian, and Usman Ali. "Efficacy of live DDoS detection with Hadoop." In NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium, pp. 488-494. IEEE, 2016.

Authors

Ms Gauri Mathur, is currently pursuing P.hd in RIMT University, Punjab. She is currently working as Assistant Professor in Lovely Professional University, Punjab. Her research areas include IoT, Wireless sensor Networks, MANETS.

Dr. Wiqas Ghai, is currently working as Associate professor in Department of computer applications at RIMT University, Punjab. He has completed Doctorate from Punjabi University Patiala. His Areas of research include nlp, plant disease detection using deep learning, computer Networking.

RESEARCH ARTICLE

How to cite this article:

Gauri Mathur, Wiqas Ghai, “A Novel Technique for Blackhole Discernment Employing Big Data Analytics in IoT Networks”, International Journal of Computer Networks and Applications (IJCNA), 8(5), PP: 682-692, 2021, DOI: 10.22247/ijcna/2021/209995.