Dynamic Blackhole Grayhole detection for IoT devices connected using DTN

Afroze Ansari, Mohammed Abdul Waheed

Center for Regional Studies, Regional Office
Visvesvaraya Technological University, Kalaburgi, India
ansariafroze@yahoo.com

Abstract. IoT based connections are common in new era of communication and henceforth, an over sight of analysis is required to be viewed on challenges occurred under transmission channel. In this paper, a new technique is developed to assure the safer transmission of data via IoT devices connected using Delay Tolerant Network (DTN). Typically, the technique aims to detect blackhole and Grayhole attack and hostage nodes to assure early detection. The technique is first of its kind in IoT devices. The experimental results of technique are evaluated using a real-time IoT MSP431 module and the result demonstrates an accuracy of 96.07% of detection under a 64 cluster node environment of WSN.

Keywords: Empirical Wavelet Transform (EWT), Glaucoma detection, Image processing.

1 Introduction

The wireless sensor networking based communication devices and infrastructure is been modernized with growing technology. IoT based communication devices are in potential use and higher order of stability to perform and validate the overall system behavior via communication channels. The stability analysis is achieved with the introduction of IoT technology and hence forth the dependencies of node data transfer are interdependent via multiple servers and communication devices. These devices are improved from internal offline or limited space operation to online mode of operation. Thus IoT technology improves overall stability of networking environment and devices.

The major research challenge in terms of security and stability of the system operation is the early detection or prediction of black hole and gray hole attacked nodes. These nodes are tampered nodes and hence a leveling orientation is always a challenging task. The primacy nodes and operation protocols of IoT environment aims to provide a larger space for evaluation and expansion with respect to the node and its application. The application demand of an IoT system is improvising on each passing day and growing technological advancements. These applications are developed into a primary sector of evaluation and thus results with an add-on feature for evaluation.

ICASISET 2020, May 16-17, Chennai, India

DOI 10.4108/eai.16-5-2020.2304036

The research challenge is when these nodes are inter-combined with each other without the mature dependency evaluation [4].

On a larger front, the developed application based on IoT is operational on primary applications and hence it is paired to the similar operating system of IoT devices to assure the maximum performance benefits and higher order of service. During these processes of pairing and attribute sharing, the functional and security aspects of IoT devices are compromised on backend. These attribute can corrupt the operation of a node via malfunctioning and entering into an ideal state of operation with blocking the information transfer chain. Hence resulting in the formation of unevaluated node such as gray hole and black hole. These unattended nodes are major causes of delay instruction in the chain of information management.

In this article, a new technique is proposed to evaluate and calibrated the contributions of IoT devices with respect to the trivial WSN network in formation and detection of black holes and gray holes respectively. The technique is first of its kind to understand the phenomenal operation of these clustered nodes in IoT environment. As today, the dependencies of IoT are intensively improving across all domains of operations and applications. The technique aims to attain a higher order of performance as these malicious nodes are eliminated and detected before the damage is done to the networking environment.

2 Literature Survey.

The IoT devices are considered boon for communication application and WSN based device operations. These devices are typically interconnected to form an oral of network towards assuring the operation and completion of task basically information transmission. These devices exercise a delay in information transmission and hence an interpreter is evaluated to understand the basic need of information tampering and information blocking. The information blocking is typically due to the node operational delay tolerance and node ideal state of operation. i.e the nodes are typically operational to one front of information receiving but is un-operational towards information sending or passing to the other progressive nodes in the line of communication. Hence such nodes are to be addressed and rectified before the damage in networking performance. Ali S.M.A. et.al [1] has discussed the detection of blackhole and grayholes under a constructive infrastructure to monitor the operation of information transmission over IoE (Internet of Everything) and IoT.

Typically, the devices under IoT based on cross layer architecture is disused by Sethi. A. et.al [2], the technique is proposed over the IoT devices based on NGN to assure the stability factor of operation in the environment and uphold the transmission ratio over the blocking nodes. Mabodi. et.al [3] has discussed a technique to assure a safe performance of IoT devices over the cryptographic authentication schema of multi-level [6] [8]trusted based intelligence. The technique claims 94.5% of accuracy in detecting the Grayhole attack in launch. The overall need of such techniques is to assure a safe and dependable module evaluation of IoT devices [5][9].

3 Methodology

The proposed technique is aimed to perform a dynamic evaluation of blackhole and Grayhole attack detection in the IoT based devices. These devices are calibrated and hence a dynamic evaluation approach is required for scalable implementation as shown in Fig.1.

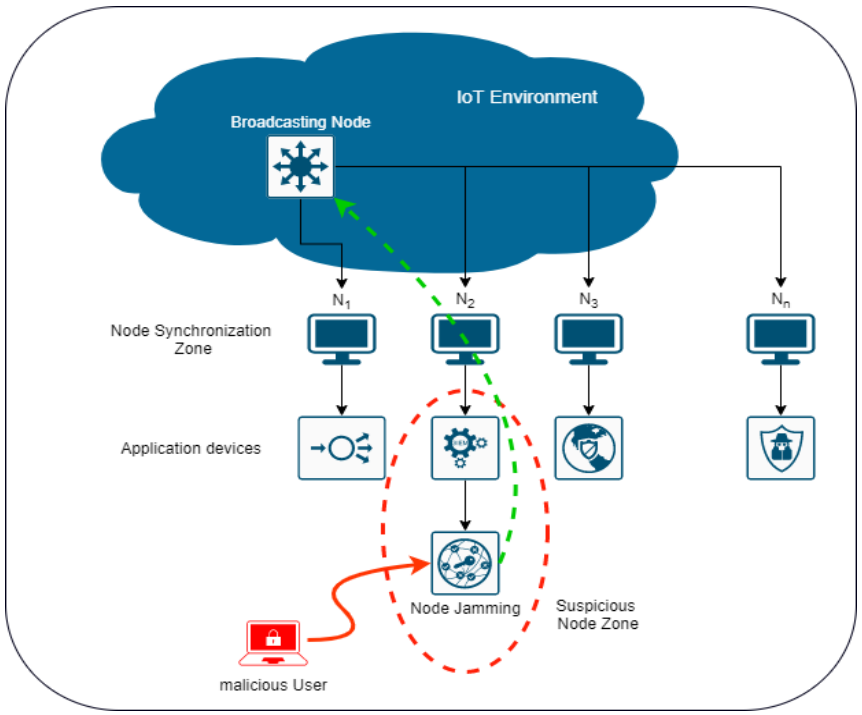

Fig. 1: Proposed System Architecture diagram

In the proposed system, the broadcasting nodes are calibrated with interconnected nodes for operation enhancements and data synchronization. The broadcasting node typically, controls the subordinate node such as $\{N_1, N_2, N_3 \ldots. N_n\}$ the universal set of devices controlled and coordinated under single node of operation and monitoring. Under these scenarios of operation, the malicious node is identified and attacked as shown as malicious user in Fig. 1, these users control the operation of application based system connected to IoT cloud and hence a terminology of grayhole and black-hole is originated.

Thus these nodes are further related to operate under single line of coordination as shown in red dots. The zone is termed as suspicious node zone. Typically, for a broadcasting node, the location and malicious user identification is hidden [7] and hence the alert is generated when the user system encounters information tampering or hindering as shown in Fig.2.

The idea of Fig. 2 is to assure the collection of data system and information of transmission under a closed bounce back looping system, in this system, the information is reversed and sent back to originating node and thus recording the assurance for completing a cycle. If the node information is not received under a sue course of time, the broadcasting node automatically, or dynamically generates an alert of corruption or malicious activities. These activates are further summarized in Fig. 3, towards coordinating the information collection of malicious nodes and users.

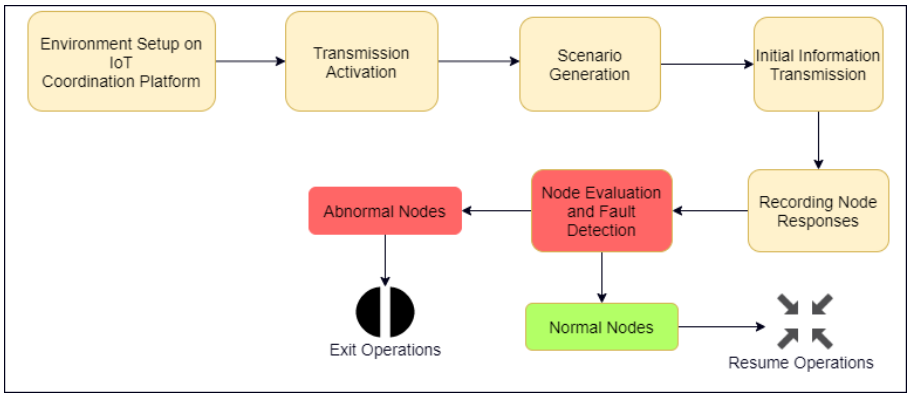

Fig. 2: Flow diagram of IoT based blackhole / grayhole node detection

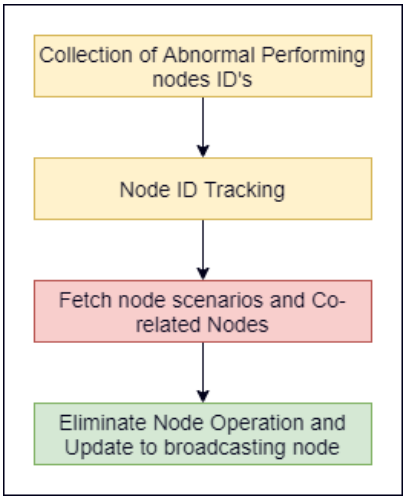

Fig.3: Blackhole / Grayhole attack re-validation with IoT devices

4 RESULTS AND DISCUSSIONS

The dynamic technique makes the system predictable and reliable on third party external devices; these devices are automatically segregated and fit into the operation mode of system behavioral approaches. Under normal mode of operation, the devices are auto synchronized to assure system normal operations by automatically reporting the cycle of information broadcasted. Under Abnormal operation performs under the control and coordination of malicious user's instructions and hence the reporting is delay as the coordination is hampered.

The performance of these devices can be validated on the dropping rate of information under normal and abnormal mode of operations. These operations are restricted and hence by the proposed technique, the evaluation of devices in longer distance can be resolved via continues mode of information cycle reporting. As shown in Table. 1. The data presents a clear understanding on various parameters such as device location, attribute coordination support and highlighting parameters such as name, cluster information and dropping rate is projected. The evaluation is further strengthening by operational transmission cycle mode.

Table. 1: Evaluation parameters of proposed technique.

Device Type	Location Scale	Cluster Mode	Bandwidth Support (mbps)	Dropping rate (mpbs)	Transmission Cycle Delay (ms)	Statusof operation
User node	IoT unit	Normal	100	2	0.34	Normal
User node	Supporting unit	Normal	150	7	0.421	Normal
User node	IoT Unit	Medium	100	2	0.45	Normal
User node	Supporting unit	Medium	150	7	0.587	Normal
User node	IoT Unit	High	100	2	0.651	Normal
User node	Supporting unit	High	150	7	0.843	Normal
User node	IoT unit	Normal	100	2	0.467	Abnormal
User node	Supporting unit	Normal	150	7	0.629	Abnormal
User node	IoT Unit	Medium	100	2	0.742	Abnormal
User node	Supporting unit	Medium	150	7	0.729	Abnormal
User node	IoT Unit	High	100	2	0.823	Abnormal

User node	Supporting unit	High	150	7	0.932	Abnormal

5 CONCLUSION

The dynamic technique for detection of blackhole and grayhole under IoT devices is first of its kind in research domain. The technique differentiates a node's based on operation and performance of interconnected devices. These devices are correlated under a cycle information transmission. These transmission are aimed to detect and validate normal operation mode of system nodes and hence based on reverse tracing, the malicious user identification can be retrieved. In near future, the proposed scheme can be appended on node attributes under mobile operations and applications connected via IoT cloud.

References

1. Ali, Shoukat, Muazzam A. Khan, Jawad Ahmad, Asad W. Malik, and AnisurRehman. "Detection and prevention of Black Hole Attacks in IOT & WSN." In 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), pp. 217-226. IEEE, 2018.
2. Sethi, Anita, Sandip Vijay, and Anurag Aeron. "Secure cross layer architecture for IOT devices in NGN." IJRTE 8, no. 1, pp. 2533-2537. 2019
3. Mabodi, K., Yusefi, M., Zandiyan, S., Irankhah, L. and Fotohi, R., 2020. Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication. The Journal of Supercomputing, pp.1-26.
4. Sherasiya, T., Upadhyay, H. and Patel, H.B., 2016. A survey: Intrusion detection system for internet of things. International Journal of Computer Science and Engineering (IJCSE), 5(2), pp.91-98.
5. Ahmed, S.T., Sandhya, M. & Sankar, S. TelMED: Dynamic User Clustering Resource Allocation Technique for MooM Datasets Under Optimizing Telemedicine Network. Wireless PersCommun 112, 1061–1077 (2020). https://doi.org/10.1007/s11277-020-07091-x
6. Ahmed, S.T., Sankar, S. & Sandhya, M. Multi-objective optimal medical data informatics standardization and processing technique for telemedicine via machine learning approach. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02016-9
7. S. T. Ahmed and S. Sankar, "Investigative Protocol Design of Layer Optimized Image Compression in Telemedicine Environment", Procedia Computer Science, vol. 167, pp. 2617-2622, 2020, [online] Available: https://doi.org/10.1016/j.procs.2020.03.323
8. Dafni Rose J, Vijayakumar K, "Data Transmission Using Multiple Medium Concurrently", IJET,2018.
9. K. Vijayakumar, S. Suchitra and P. Swathi Shri, "A secured cloud storage auditing with empirical outsourcing of key updates", Int. J. Reasoning-based Intelligent Systems, Vol. 11, No. 2, 2019.