J. Sustain. Wireless Syst., vol. 02, no. 3, pp. 133-137
https://doi.org/10.36548/jsws.2020.3.005

Wireless IoT with Blockchain-Enabled Technology amidst Attacks

Dr. Khaled Kamel,
Professor,
Department of Computer Science,
College of Science,
engineering and Technology,
Texas Southern University,
USA.
Email: Khaled.Kamel@tsu.edu

Abstract- Blockchain enabled Internet of Things has exhibited high potential in establishing consensus and trust mechanism. To design this type of system, it is necessary to have a better knowledge about blockchain and how it can be used with internet of things. Moreover, it will be easier to gauge the requirements of the system based on the performance constraints that are imposed on the other parts. In the proposed work, we have used spatial domain Poisson distribution to determine the arrival rate at the transaction node and the full function node. The signal to interference and noise is calculated to determine throughput as well as transmission success rate. Based on performance analysis, we have developed an algorithm that is can be used to determine the apt FN deployment, under the condition of maximum transaction throughput. Results indicate the accuracy of the proposed algorithm with theoretical values.

Keywords: IoT; Blockchain; security; throughput; Attacks

1. Introduction

Internet of Things (IoT) is an evolutionary technology that continues to introduce advancement in devices and machines on a global scale, transforming the way we live. Playing such a crucial role, breaching such a technology will create havoc in our lives and securing it is of highest priority. This is especially hard since it is easy to access and the constraints on software/hardware [1-4]. There is much focus on the cost need and effort to detect the vulnerability of such systems and prevent any attack that comes its way. When IoT is involved, a cloud server becomes mandatory for the purpose of authorization, identification and further communication with other devices which will result in increasing the expenditure for using and maintaining the cloud. Since the use of a centralized IoT is not possible for smaller companies, other third parties are involved, thereby increasing the cost consideration of the system which makes it an unattractive option for the consumers [5].

To handle these issues, blockchain has been developed, to ensure that there is no security and trust issues when using IoT. Blockchain is the basic algorithm that is used in a number of revolutionary projects such as bitcoin [6-7]. Here the information is saved in the form of data blocks and as there is increase in information, the number of data blocks keeps increasing. Every data block that is generated is built with the help of certain algorithms that are used to define their operation. However, there are some principles that are to be followed when blockchain technology is involved which enables them to ensure highly safe transaction, cost effective and progressive [8]. This makes it a key aspect that helps overcome the discrepancies present in IoT. Moreover, the use of blockchain removes the need for third part intervention when two smart devices are connected to each other. In fact, a survey shows that in 2025 more than 35% of the IoT systems deployed will be using blockchain services [9]. However, the drawback with using blockchain and IoT together is the need for memory space, computing capability and power supplement which might result in an increase cost consideration. Hence there has been much focus on blockchain design which excel in terms of privacy, trust and consensus mechanism compromising on an efficient network architecture to introduce a wireless IoT system built on blockchain [10].
Over the years, research has been carried out on traditional wireless network. However, these analysis methods cannot be use to examine the performance of recent wireless network modelling, mainly due to the introduction of blockchain technology. In [11] and [12] the researchers have made use of stochastic geometry to determine how well traditional networks perform in terms of outage probability, throughput and association probability. However, these analyses are made without taking into consideration time domain and focussing largely on spatial domain. For an efficient blockchain based IoT system, communication performance and security performance should be of high reliability in order to prevent and sustain when attacks occur.

ISSN: 2582-3167
Submitted: 18.12.2020
Accepted: 22.12.2020
Published: 02.01.2021

J. Sustain. Wireless Syst., vol. 02, no. 3, pp. 133-137
https://doi.org/10.36548/jsws.2020.3.005

In this proposed work we define a novel network model which can be aptly implemented in IoT systems with the help of blockchain technology. In this work, based on the requirement, full function nodes are deployed into the environment such that when there is need for extra support, the blockchain is enabled [13].

2. Wireless Communication Model

A typical blockchain enabled IoT model with spatio-temporal domain characteristics are used as reference for the wireless communication model. Consider an area 'A' with full function nodes (FNs) and IoT transaction nodes (TNs) which are distributed in the form of homogenous PPP with densities λ_f and λ_d. We assume that the distance between FN and TN is d and the minimum distance is d_{min}. Based on the distance between TN and FN, the association rule is frame. When a transaction arrives at a particular transaction node, it should get ready to broadcast the data by entering into the active mode. The length of the transaction packet is specific and will be able to hold only 2 transaction nodes at a time. Hence in general, for different transmission range, the size of the data packet is also set accordingly. Similarly, the traffic arrival rate can vary anywhere between few to several hours. The arrived transactions can be performed using λ_f, which is a Poisson distribution, T.
As far as a wireless channel is concerned, we take into consideration a TN that is served by FN. While travelling, there is a possibility of interference and path loss is experienced by the signal contributed highly by the active TN. The Signal to interference and noise ratio can be determined using the following expression:

$$SINR(A_1, N_1, A_2) = \frac{Pg(A_1)}{\sum_{t=1}^{N_1} Pg\left(A_2^{(i)}\right) + \sigma}$$

Here P is the power of all the transaction nodes (TN), A represents the radius and the distance between FN and TN is A_1 while A_2 can be represented as $A_2 = [A_2^{(1)}, A_2^{(2)}, \ldots., A_2^{(N_1)}]$. σ is the noise power and N_1 denotes the total interferences TNs. A_0 is the radius of distance between FN and the transaction node as shown in Fig.1.

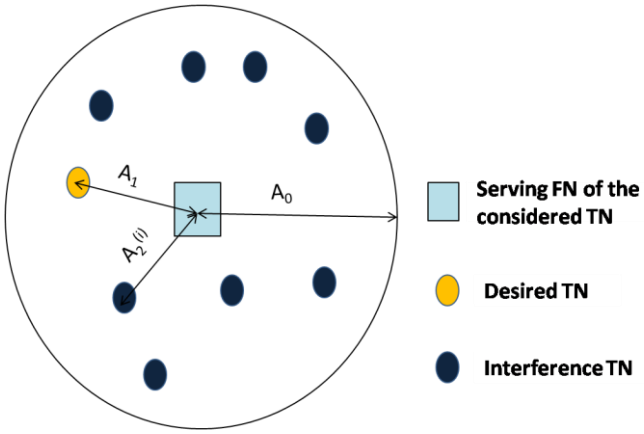

Fig 1. Interference are for a Transaction Node

3. Blockchain-enabled IoT Model

Full function nodes and transaction nodes are said to be two major elements. FNs are used for their storage capacity and computing power. They have the capacity to support blockchain characteristics in order to take control over building new blocks, data storage and transaction confirmation. Using wireless communication as well as independent interface, the FNs are connected together. On the other hand, the TNs are simple systems that support IoT devices enabled by the blockchain system Wireless communications also serves as a link between the TNs and FNs. Important information is transacted between the TNs and are further saved as blocks, on confirmation by the FNs. When information reaches a transaction node, it is broadcasted to reach the FNs with the help of IoT.

A typical transaction process involves the following key characteristics:

- Wireless IoT networks are used to broadcast data to the FNs when a transaction arrives at a particular TN.
- In general, this information should be received by multiple FNs to increase the level of security. In this paper, we have implemented reception in only one FN.
- From this FN, information is passed to all the other FNs by means of dedicated connections.
- The transacted information is now built into a block by the FN and all the other FNs are also made to update their transaction aspects accordingly.

ISSN: 2582-3167
Submitted: 18.12.2020
Accepted: 22.12.2020
Published: 02.01.2021

Fig.1. represents a simple block-chain enabled IoT model. In this model relationship between FNs and TNs, active FNs and active TNs are said to be dynamic with respect to time. We take into assumption that there are certain harmful or infected FN nodes present in the network. However, the ratio of nodes that are harmful is less than 50% of those that are secure and reliable. If a FN is malicious, it might result in making a Denial-of-Service attack, in which case, the FN is considered to be in 'OFF' mode and another nearby FN is searched for. Similarly, if a harmful FN tries to interfere with the data transacted, the signature will not be validated, thereby blocking the FN. Because of this, a TN will look to choose any other FN when transaction is incomplete.

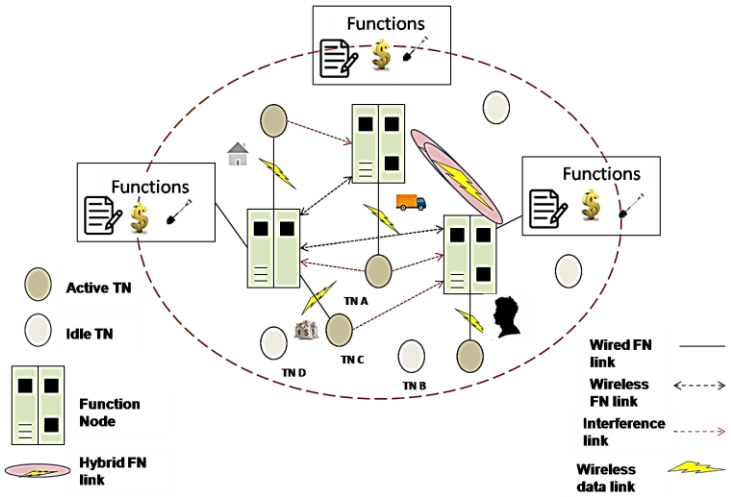

Fig.2. IoT system model with Blockchain

The FNs can be connected by means of wireless and wired hybrid relay link, wireless point to point link and wired link. Depending on the surrounding of the FNs, this connection will vary as represented in Fig.1. When the FNs are close to each other, one can use the wireless link and when they are farther away from each other, wired link is preferred in order to avoid external environmental interferences. For a more cost-effective and efficient system, a hybrid connection of wired and wireless links are used, based on the IoT network's range.

4. Results and Discussion

The security performance of the proposed work is analyzed by imposing three typical attacks namely random FN attack, random link attack and eclipse attack. We have examined the overall throughput of the proposed work with respect to the three attacks and it is found that it reduced by 10% from its output without the attack as shown in Fig.3(a). Here, a dip of 10% is observed because once a particular mode is attacked it will result in affecting all the other links also.

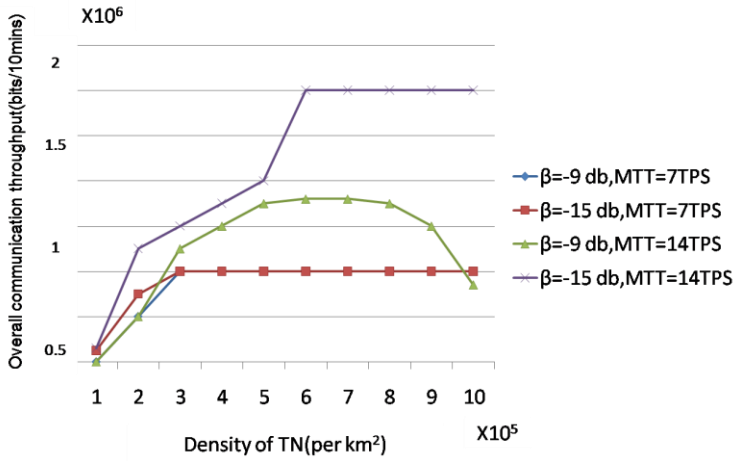

Fig.3 (a) Eclipse Attack

ISSN: 2582-3167
Submitted: 18.12.2020
Accepted: 22.12.2020
Published: 02.01.2021

Similarly, in Fig.3.(b) it is observed that the throughput is lesser than 10% since it is not possible to control TN connections by the attacker. Hence the TN is still active enough to communicate, despite degradation of the wireless channel. In Fig.3 (c), the degradation is observed to be 10%.

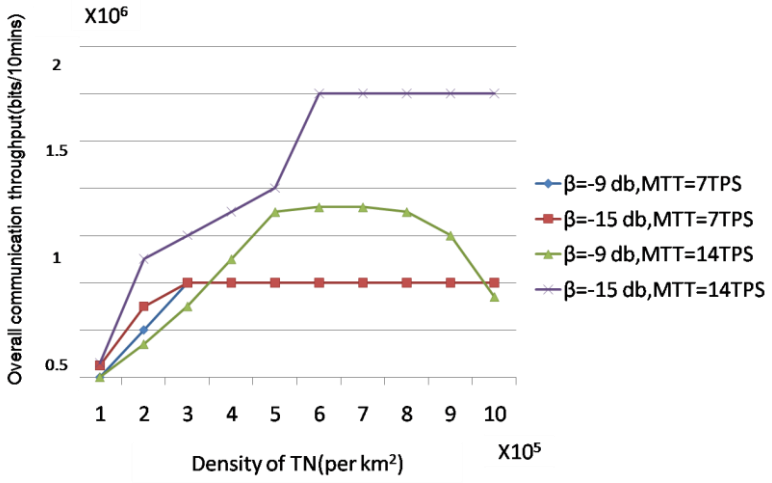

Fig.3 (b) Random link attack

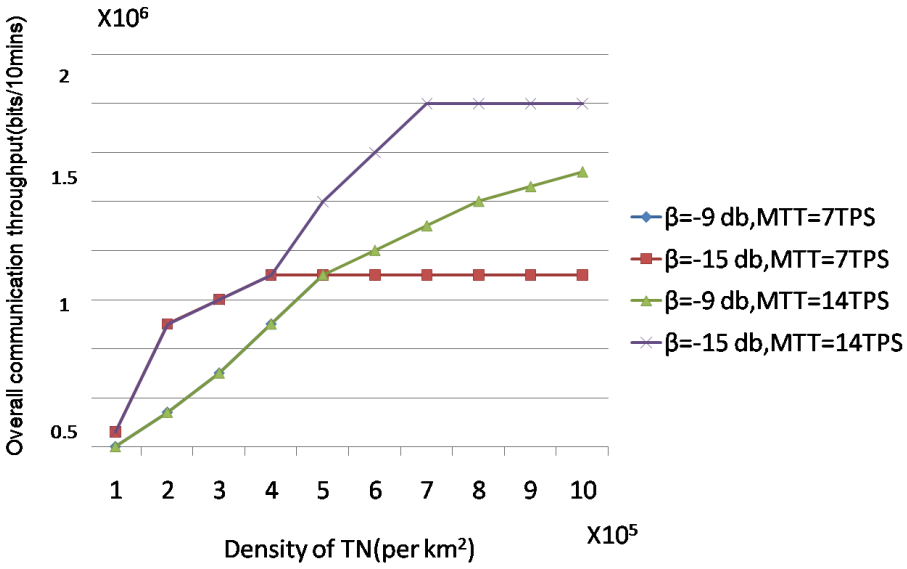

Fig.3 (c) Random TN attacks

5. Conclusion

In this paper, we have evaluated the accuracy of the proposed blockchain-enabled IoT system. In the first section of this work, theoretical analysis of the transmission successful rate, communication throughput and SINR is performed. This analysis shows that using our proposed methodology, communication throughput occurs with minimal FN and maximum transaction is also achieved. Result analysis shows that our methodology shows validation of our theoretical analysis with a difference of 5%. This proposed work provides a basic framework for introducing blockchain-enabled IoT system design. This lays the footwork for future work on algorithms, protocol designs and performance analysis. An upcoming research topic for the proposed work is the development of optimized and novel communication protocols that make used of blockchain systems-embedded broadcasting. Similarly, secure wireless blockchain system is another possible future topic that involves the use of physical layer security techniques.

ISSN: 2582-3167
Submitted: 18.12.2020
Accepted: 22.12.2020
Published: 02.01.2021

References:

[1] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, 173-190.
[2] Tsang, Y. P., Choy, K. L., Wu, C. H., Ho, G. T. S., & Lam, H. Y. (2019). Blockchain-driven IoT for food traceability with an integrated consensus mechanism. IEEE access, 7, 129000-129017.
[3] Mistry, I., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. Mechanical Systems and Signal Processing, 135, 106382.
[4] Dwivedi, A. D., Srivastava, G., Dhar, S., & Singh, R. (2019). A decentralized privacy-preserving healthcare blockchain for IoT. Sensors, 19(2), 326.
[5] Huang, J., Kong, L., Chen, G., Wu, M. Y., Liu, X., & Zeng, P. (2019). Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. IEEE Transactions on Industrial Informatics, 15(6), 3680-3689.
[6] Casado-Vara, R., Chamoso, P., De la Prieta, F., Prieto, J., & Corchado, J. M. (2019). Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management. Information Fusion, 49, 227-239.
[7] Shirley, D. R. A., Ranjani, K., Arunachalam, G., & Janeera, D. A. (2020). Automatic Distributed Gardening System Using Object Recognition and Visual Servoing. In Inventive Communication and Computational Technologies (pp. 359-369). Springer, Singapore.
[8] Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J., & Zhang, Y. (2019). A blockchain-based nonrepudiation network computing service scheme for industrial IoT. IEEE Transactions on Industrial Informatics, 15(6), 3632-3641.
[9] Rane, S. B., & Narvel, Y. A. M. (2019). Re-designing the business organization using disruptive innovations based on blockchain-IoT integrated architecture for improving agility in future Industry 4.0. Benchmarking: An International Journal.
[10] Sivaganesan, D. (2019). Block Chain Enabled Internet of Things. Journal of Information Technology, 1(01), 1-8.
[11] Alladi, T., Chamola, V., Parizi, R. M., & Choo, K. K. R. (2019). Blockchain applications for industry 4.0 and industrial IoT: A review. IEEE Access, 7, 176935-176951.
[12] Sun, Y., Zhang, L., Feng, G., Yang, B., Cao, B., & Imran, M. A. (2019). Blockchain-enabled wireless Internet of Things: Performance analysis and optimal communication node deployment. IEEE Internet of Things Journal, 6(3), 5791-5802.
[13] Xu, H., Zhang, L., Liu, Y., & Cao, B. (2020). Raft based wireless blockchain networks in the presence of malicious jamming. IEEE Wireless Communications Letters, 9(6), 817-821.

ISSN: 2582-3167
Submitted: 18.12.2020
Accepted: 22.12.2020
Published: 02.01.2021