Deep-Markove Learning Model for Consensus Scaled Optimization in Multi-Agent Systems for DDoS Attack Detection

Abstract

The main issue of distributed system is obtainin consensus on some data volume to reach to reliability in unreliable system data. There are no availabile system in perfect mode in real life. It is because of some hardware and software errors, slow networks, packet drops errors, bit error rate and noise and etc. This article deal to two other criteria in terms of quality of services and energy consumption in muti-agent systems connected to networks to optimizing consensus scaled modeling. The types of network supposed to be Internet of Things (IoT). IoT requires the creation of new structures that use edge and fog computing environments due to the lack of optimal quality of services and bandwidth requirements. This new paradigm can accomplish many of internet tasks on the edge and fog which is capable to confronting a wide range of technologies in the IoT. For example, edge and fog computing can be used in smart home, smart city, smart driving and other things that are planned based on IoT mechanisms. Since resource management along with quality of services in the IoT has been challenging in recent years as the technology has grown, providing integrated structures is essential and connecting to link quality due to more internet speed. For this purpose, Block Chain with a minimum computational complexity and high level of flexibility are provided which are capable to create gateways for the IoT -based edge and fog computation with a regular and optimal access mechanism for link quality based on deep markove model. This research aims to provide a secure routing schema with the maximum authentication of data in the connected of link quality internet environment with multiple edge and fog computing for DDoS attack detection. The use of encryption mechanisms including DTLS and FSK is considered as the main approach used in the Block Chain structure for transmitting and receiving data in variety of application. The proposed approach is called the EQoSR-IoT. Improving the quality of services includes delays, throughput, probability of data detection, probability of miss detection, and data lose rate to manage the resources of the network to create a new schema of authentication in routing is necessary. The results represented that the proposed approach has better performance in comparison to others.

Keywords: Internet of Things (IoT), Consensus Scaled, Edge and Fog Computing, Routing, Energy, Quality of Services (QoS), Deep Learning, Markov Model, DDoS Attack Detection

Introduction

The Internet of Things network is presented as the newest Internet-based computer networking model and structure. This network works as several objects communicate with each other through an array of sensors or other technologies such as Bluetooth which can send and receive data. The growth of such a network which don't need human resource intermediaries can send and receive data through objects at certain times and will surely lead to high development. This expansion on a large scale can display various challenges. A series of challenges include security, routing, clustering, reliability, and more. In this case, it is necessary to propose new and advanced solutions that operate intelligently [1]. Security is considered as the one of the most perilous challenges of the IoT. So that various objects connected to the Internet may be subjected to various cybercrime attacks and since humans do not directly interfere with the sending and receiving of data in such a network, so there may be many problems in an environment or organization and other sections. An obvious example of this is that sensors in smart homes that have remote control capabilities through the IoT can cause cyber-attacks, and overlap control settings. This can be a huge cost to users of the IoT. Therefore, providing new security solutions are essential [2].

Cryptography can solve many problems in security. Cryptography is used as a coding structure to codify data. To do this, it should have access to the main structure of the applicable programs covered by the IoT and can encrypt their data in sending and receiving. One of the structures that this research is trying to encrypt is the use of lightweight protocols. Cryptography of communication channels with lightweight protocols can be a new issue in the IoT. Creating a secure environment used with responsive schema at the level of the Constrained Application Protocol (CoAP). The use of cryptographic structures at the level of the applied data layer is based on the security mechanism of the Datagram Transport Layer Security (DTLS) with the Pre-Shared Key (PSK) [3]. Denial of Service (DoS) or Distributed Denial of Services (DDoS) are two main attacks in application layer of IoT. This research attempts to provide a secure routing regardless of the type of attack that may be used on edge and fog computing. The use of edge and fog computing in the IoT as well as cloud and fog computing can be seen on the IoT in the Figure (1).

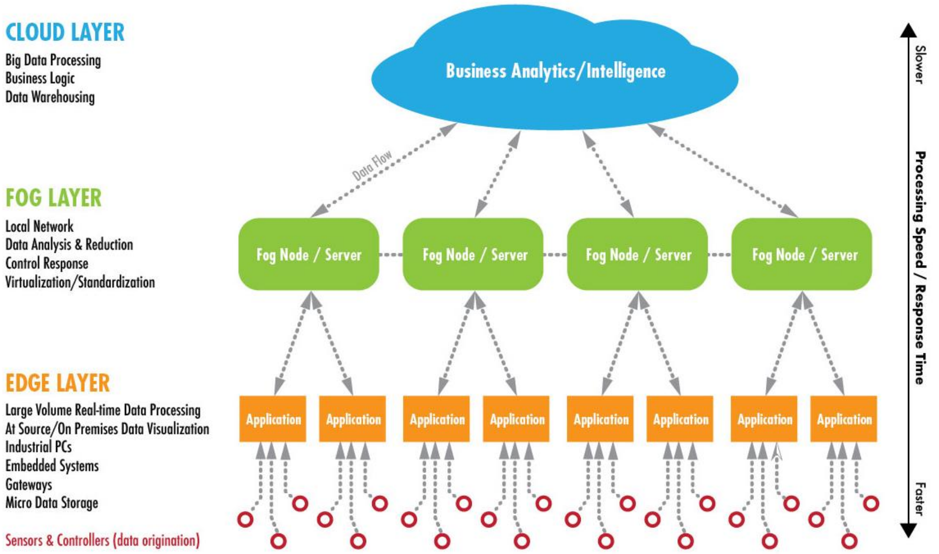

Figure (1) Cloud, fog and edge computing in IoT environment

It is expected that to create a new multi-edge secured routing on the IoT which can be provided to resource management. The purpose of resource management is the Quality of Service (QoS) which includes throughput, Bit Error Rate (BER), delay, and Signal-to-Noise Ratio (SNR). All these things will be provided and created on the safe routing. In general, the most important goals pursued by this research include:

- ✓ Presentation of a new Block Chain secured prototype model to guarantee the security of the IoT with better authentication and energy consumption.
- ✓ Providing a cryptographic model on routing based on the security mechanism of the data Datagram Transport Layer Security (DTLS) with the Pre-Shared Key (PSK) in the Block Chain in the platform of multiple edge and fog computing-based IoT as multi-agent system with deep Markov model for DDoS attack detection.

Block Chain Review

The name "Blockchain" itself refers to the structure of the Blockchain's data can be thought of as an immutable chain of events. Data, mostly in the form of transactions, is grouped together in a block. This block is then packaged with a reference to the previous block, which contains a reference to the block before that, etc. Blockchain is "distributed" because every participant in the network holds a copy of this append only ledger. All participants, or peers, must agree on the state of the ledger and unauthorized changes to that ledger must be reasonably detectable. In reality, Blockchain technology requires (1) a distributed ledger among peers, (2) a consensus protocol to ensure that all peers have the same copy, and (3) a cryptographic infrastructure. Every other detail is determined by the desired application.

A. Consensus Protocols

We provide an overarching classification for consensus methods. In-depth protocol algorithms and mathematical proofs of robustness are beyond the scope of this paper. Consensus protocols have their own massive pool of research effort and are well-reviewed in other works [4]:

1) Lottery Election: Lottery election, such as Proof ofWork (PoW), relies on probability to “elect” a consensus leader who determines the order of incoming transactions, usually for a set amount of time. In Bitcoin, peer nodes append a nonce to a block and calculate the hash value. The resulting value must have some pre-determined number of leading zeros. Peers constantly hash new values in order to find the correct “answer.” The first peer to find the right nonce broadcasts its results to the network, who verifies and appends the block organized by the winning leader. This temporary leader is the one that determines the order of transactions within its announced block. In this case, difficulty is determined by the number of leading zeros and the leader is only the leader for one block. Other lottery election examples include Proof of Stake (PoS) and Proof of Elapsed Time (PoET) [4], although this is by no means an exhaustive list. Note that election difficulty and leader term lengths could be configurable parameters.
2) Majority Election: Majority election refers to a majority of peers voting on a particular value. Peers could vote to validate a transaction, or vote upon a block leader. The distinction here is that majority election does not rely on probability, but is instead far more communication-bound - the notable example being Practical Byzantine Fault Tolerance (PBFT) [5]. Consensus in this manner must take care to manage its upscaling to prevent significant communication overhead. The general trend is to create “round robin” or subgroup voting pools to mitigate scaling issues [6].

B. Implementation Differences

1) Read-Write Access: Blockchain systems can be defined by what entities have read and write access to the ledger. As aforementioned, write access is append-only. If any peer can read the ledger, it is public. If the read access is limited, it is private. If any peer can append to the ledger, it is permission less. If write access is limited, it is permissioned. Bitcoin serves as the prime example of a public, permission less Blockchain network. Anyone can participate in the network and the ledger is open to the public. Anonymity is preserved by the use of public-private key pairs. Public networks tend to require computationally heavy consensus methods - or, in the case of Ethereum’s ethash method [7], computation and memory-intensive. This is mainly to protect against Sybil attacks and prevent double-spending (see II-C). A network like Sovrin [8] is public and permissioned. Anyone has access to ledger information, but additions to the ledger can only be made by specific set of participants. Permissioned Blockchain have the benefit of not requiring consensus methods as resource-intensive as permission-less systems, since unauthorized parties could be revoked for not being part of a whitelist. Privacy is not a goal for Sovrin, which is an identity management system. Alas, even for Bitcoin’s anonymous addressing, true privacy is not guaranteed on a public network [9]. Private, permissioned Blockchain like Hyperledger Fabric [10] target enterprise applications, where businesses may want the fault tolerance and self-management offered by Blockchain within a private network. Smaller networks reduce communication overhead, but tend to be less secure as a result - large, public networks have the advantage of peer numbers, where a 51 percent majority attack is more difficult to execute.
2) Block Handling: Block handling refers to methods which try to reduce Blockchain latencies, either in writing to the ledger or reading from it for transaction validation. These methods include block ordering, pruning, and ledger sharing. Block ordering can be handled in a number of ways. Bitcoin can result in forks - when more than one peer concurrently broadcasts a valid block to append to the ledger. At that point, peers will continue to “race” against one another to find the next hash value, and once the longer chain is created, the other peers will adopt that chain. Ethereum mitigates this wasted effort by creating incentives to include so-called “orphaned” blocks into the main chain. Directed Acyclic Graphs (DAG) have also been suggested for block ordering to decrease ordering delay [11, 12]. Whereas traditional Blockchain are mostly linear in structure, DAG Blockchain allow for more complex web chains. Block pruning has been suggested to reduce ledger size [13] [14], generally by reducing older blocks into a new “jumpoff” point from which the ledger can continue. As long as all peers reach consensus and agree to prune, the ledger can be collectively reduced. This method needs to carefully define at which point old data is considered “old enough.” Ledger sharing is another method to reduce ledger read times. A system could provide service-specific Blockchain, such as in [13-15]. Transaction validations would avoid searching through unnecessary blocks in order to find relevant information, but be linked at common blocks for some set interval. Other proposed protocols with ledger sharing can be found in [15-20].

Possible attack vectors on a Blockchain network. Which the peer node outside the inner shaded area is the only non-malicious actor presented in Figure (2).

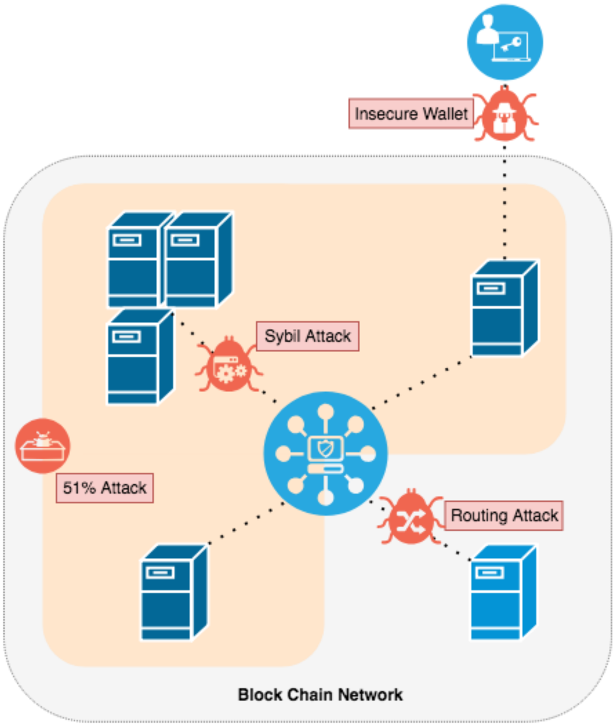

Figure (2) Possible attack vectors on a Blockchain network. In this case, the peer node outside the inner shaded area is the only non-malicious actor.

Simulation and Results

MATLAB used as simulation platform to implement the proposed approach. Due to simplicity of coding in MATLAB, it used instead of powerful simulation tools such as NS-3, NS-2, OPNet, OMNet++, GloMoSIM, JSIM, IoTSIM and so on. Also some evaluation criteria used to guarantee the proposed approach and comparison to other methods. Initial structure for IoT is necessary in simulation. It is essential to provide a basic dimension to the IoT. Defining parameters in simulation worlds is too important to examine the proposed approach and results in a concrete manner in order to obtain assumptions and goals from it. In the simulation world, defining the dimensions of a grid means that it will not be covered outside of it, but in the real world, using the tools and the equipment, the uncovered points can be partly close to the coverage range. The Table (2), shows the initial values for the general settings of the IoT, including the number of sensor nodes (which includes equipment such as Bluetooth, etc. for communication with the IoT), sampling rate, primary energy, network dimensions, etc. and adjusts their initial parameters with empirical visibility.

Table (2), initial settings of IoT network

X and Y dimension supported in IoT area	$100 \times 100 \text{ m}^2$
Sensor nodes number in IoT	300 nodes
Package number in IoT to transmit	100 packages
Maximum size of packages in IoT to transmit	100 MB
Minimum size of packages in IoT to transmit	1 KB
Sampling time in seconds	8 seconds
Initial SNR in transmitting and receiving data	5 dB
SNR range based on drop in transmitting and receiving data	20 – 20 dB
Nodes deployment in IoT environment	Random
Modulation for transmitting and receiving data	BPSK
Block Chain initial threshold in fault tolerance time	0.1
Energy of each nodes	1 Joule
Total energy of IoT	300 nodes × 1 Joule = 300 Joule

Probability of detection of DDoS attack and data privacy considered in IoT-edge-fog routing used deep Markov model which presented in Figure (4).

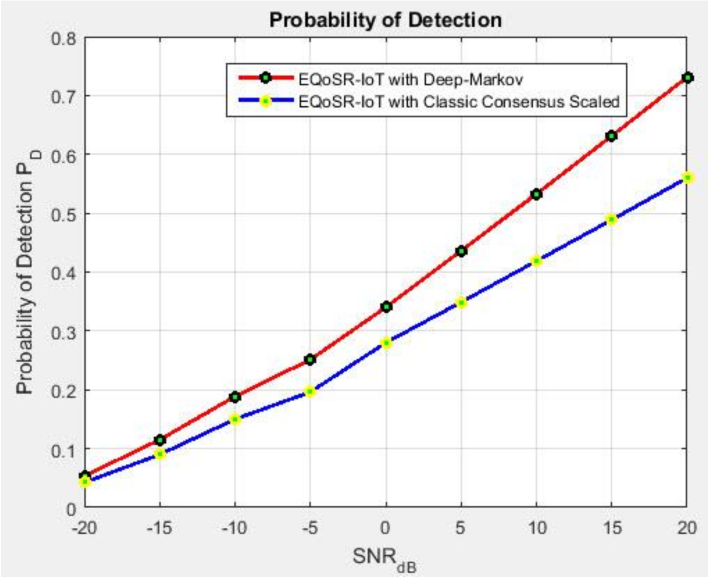

Figure (4) Probability of detection output for encrypted data to data privacy in routing

According to Figure (4), it is clear that the proposed approach EQoSR-IoT connected to deep Markov protocol has a better probability of detection capability than EQoSR-IoT used classic consensus model in the routing. The highest probability of detection is the superiority criterion. The proposed method has added more capabilities to the EQoSR-IoT connected to 5G to maintain the confidentiality of data at the time of their probability of detection. Also Probability of Miss Detection (PMD) in encryption consider (which could be due to the existence of severe noise and interruption in the IoT-based edge-fog computing) which can be affect in lost data rate and preventing its privacy. The lower probability of miss detection can be guaranteed to improve the loss data rate. Figure (5) represent the probability of miss detection of EQoSR-IoT used deep Markov model.

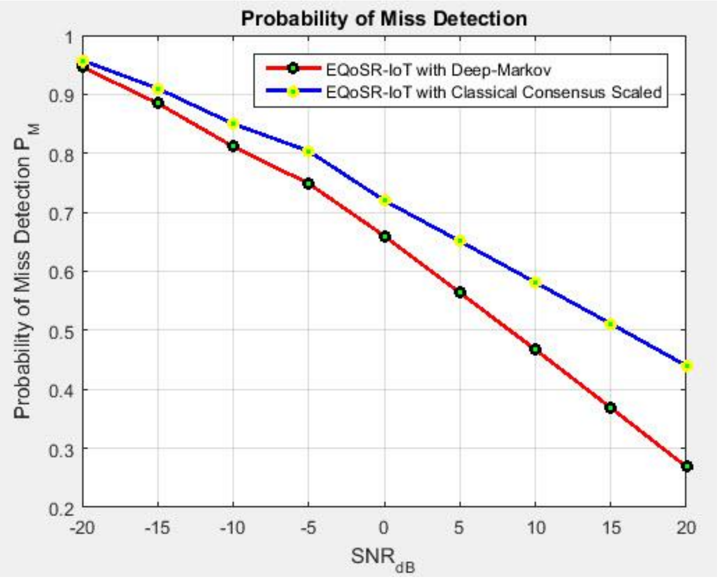

Figure (5) Probability of miss detection

It is shown in Figure (5), that the proposed approach EQoSR-IoT connected to deep-Markov has the better probability of miss detection than the EQoSR-IoT used classical consensus scaled model in the routing. The structure of DTLS and FSK in this section have also had a significant impact on the EQoSR-IoT used deep Markov model during the encryption of data in the BPSK-based messaging channel. The result of this section shows that the proposed EQoSR-IoT connected to deep-Markov method has a functional superiority in minimizing the probability of miss detection. This can certainly prove to be as low as possible to reduce the data loss rate in transmitting them from origin to destination in the context of the IoT-based edge-fog computing routing. Figure (6) shows the data loss rate of EQoSR-IoT used deep-Markov model.

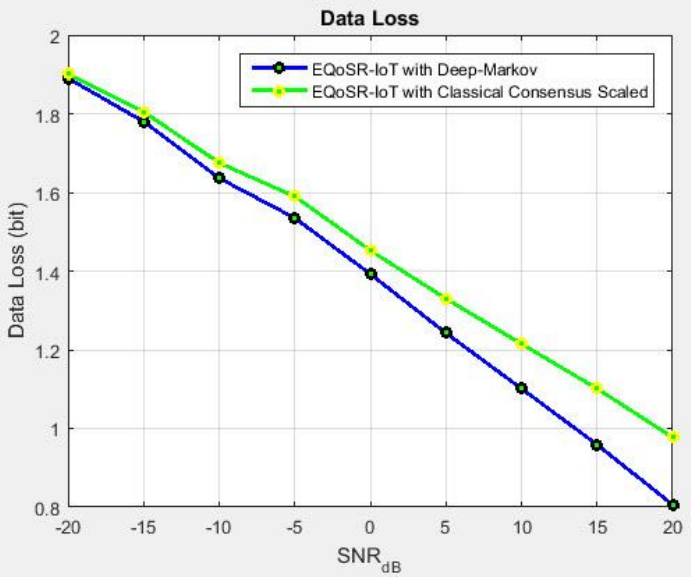

Figure (6) Data lose rate

Based on Figure (6) and the previous description, the proposed approach EQoSR-IoT has equal data loss rate with the classical consensus scaled routing model, but EQoSR-IoT used deep-Markov model is lower than that. The combined structure of the DTLS and FSK in this section, as well as the probability of miss detection, have shown their high ability. It should be noted that the data loss rate in the EQoSR-IoT used deep-Markov model communication is desirable, but may be different at the time of encryption in this study with 8 bits of information in the BPSK modulation-based communication channels. It should be assumed that the upcoming chart proves this. In the following, after creating a safe environment, quality of services criteria to evaluation consider. Initially, it is considered that the delay in Figure (7) which represent the delay after applying the proposed approach for the secure routing on the IoT-based edge-fog computing compared to the EQoSR-IoT classic model of routing.

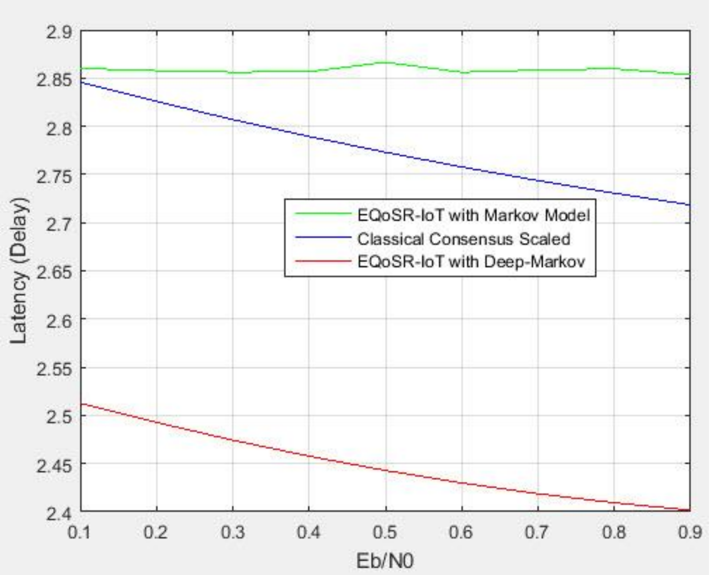

Figure (7) Delay of proposed approach in comparison to others

In Figure (7), the delay diagram of the proposed red-color scheme is characterized by a lower delay rate than the previous two methods including the EQoSR-IoT classical consensus scaled model and the Markov model routing way in the same conditions. In the following, examination of the amount of data transmitted in bits considered. If the environment is secure, the data is decoded by the DTLS and FSK-based encryption, in the sender, encrypted and in the receiver. The results of the throughput in the IoT-based edge-fog computing routing for EQoSR-IoT used deep-Markov model protocols represent in Figure (8).

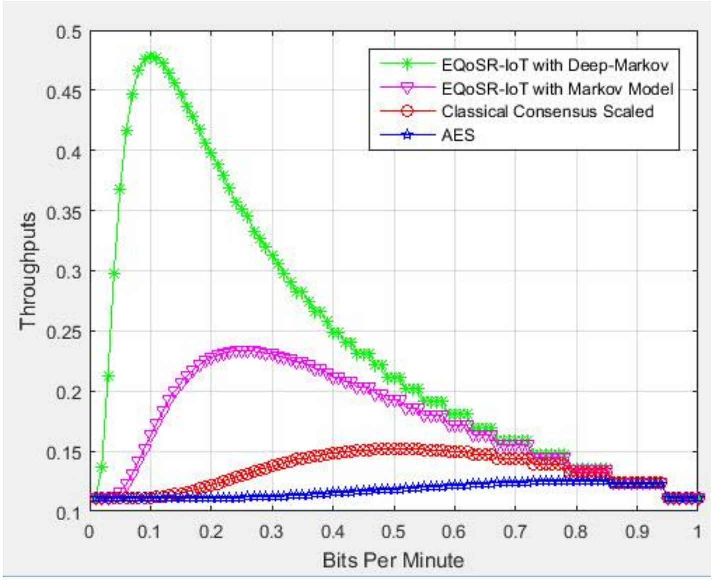

Figure (8) Throughput rate for proposed approach in comparison to others

According to Figure (8), which is compared with the EQoSR-IoT used Markov model, the classic consensus scaled model and the use of the AES algorithm, it is shown that the green graph has a higher permeability rate than the other methods. But over time, this rate is declining and is roughly the same in other ways. Figure (9) shows the proposed bandwidth results approach in comparison to EQoSR-IoT used deep-Markov model, the classic model and the use of the AES algorithm.

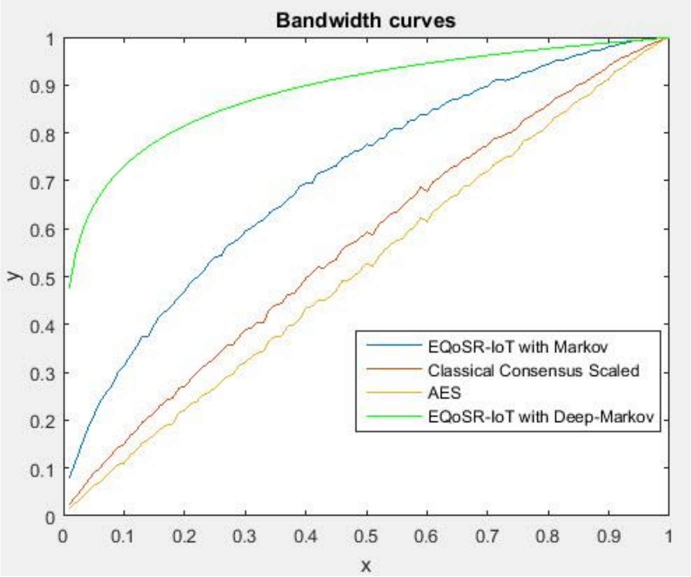

Figure (9) Proposed method bandwidth curve in comparison to other methods

Based on Fig. 9., represented that proposed method has better bandwidth curve in comparison to others. A secure routing created based on DTLS and FSK in IoT-based edge-fog computing which represented that this routing has good performance of quality of services to manage resources which cause more reliability of IoT as multi-agent system for consensus scaled.

Conclusion

In this research, the EQoSR-IoT introduced as consensus scaled model in muli-agent systems. IoT platfom used as multi-agent systems in network model for more reliability in terms of quality of services and energy consumption as new approach. The performance of EQoSR-IoT in IoT-based edge-fog computing environment was tested in simulation to detect DDoS attack. DTLS and FSK-based encryption operations are performed on a Block Chain platform in the structure of this routing. The flexibility and improvement of the EQoSR-IoT connected to RPL protocol vs. EQoSR-IoT connected to used deep Markov model efficiency can be determined by considering resource management and quality of service criteria including delay, throughput, probability of detection, the probability of miss detection and data loss rate. Of course, as improvements are made in these cases, there may be some other weaknesses that can be considered as their future solutions.

References

[1] Hugh Boyes, Bil Hallaq, Joe Cunningham, and Tim Watson. The industrial internet of things (IIoT): An analysis framework. Computers in Industry, Volume 101, Pages 1-12, October 2018.

[2] Kewei Sha, Wei Wei, T. Andrew Yang, Zhiwei Wang, and Weisong Shi. On security challenges and open issues in Internet of Things. Future Generation Computer Systems, Volume 83, Pages 326-337, June 2018.

[3] Libing Wu, Biwen Chen, Kim-Kwang Raymond Choo, and Debiao He. Efficient and secure searchable encryption protocol for cloud-based Internet of Things. Journal of Parallel and Distributed Computing, Volume 111, Pages 152-161, January 2018.

[4] C. Cachin and M. Vukoli`c, “Blockchain consensus protocols in the wild,” 2017.

[5] M. Castro and B. Liskov, “Practical byzantine fault tolerance and proactive recovery,” in Proceedings of the Third Symposium on Operating Systems Design and Implementation, Vol. 20, ACM, November 2002.

[6] D. Mazi`eres, “The stellar consensus protocol: A federated model for internet-level consensus,” tech. rep., Stellar Development Foundation, 2016.

[7] “A next-generation smart contract and decentralized application platform,” 2017. https://github.com/ethereum/wiki/wiki/White-Paper.

[8] P. Windley and D. Reed, “Sovrin: A protocol and token for selfsovereign identity and decentralized trust,” tech. rep., Sovrin Foundation, 2018.

[9] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, “Zerocash: Decentralized anonymous payments from bitcoin,” in IEEE Symposium on Security and Privacy, 2014.

[10] “Hyperledger fabric,” 2015. https://hyperledger.org/projects/fabric.

[11] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, “Inclusive block chain protocols,” in Financial Cryptography, pp. 528–547, 2015.

[12] S. Popov, “The tangle,” tech. rep., IOTA, 2017.

[13] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, “Omniledger: A secure, scale-out, decentralized ledger via sharding,” IACR Cryptology ePrint Archive, vol. 2017, p. 406, 2017.

[14] A. E. Gencer, R. van Renesse, and E. G. Sirer, “Service-oriented sharding with aspen,” 2016.

[15] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, and G. Danezis, “Chainspace: A sharded smart contracts platform,” 2017.

[16] L. Luu, V. Narayanan, C. Zheng, J. Bajewa, S. Gilbert, and P. Saxena,“A secure sharding protocol for open blockchains,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, no. 17-30 in CCS -16, 2016.

[7] Moustafa M. Nasralla, Nabeel Khan, and Maria G. Martini. Content-aware downlink scheduling for LTE wireless systems: A survey and performance comparison of key approaches. Computer Communications, Volume 130, Pages 78-100, October 2018.

[18] L. R. Priya, and K. Rubasoundar. LTE: An Enhanced Hybrid Domain Downlink Scheduling. Cognitive Systems Research, In press, accepted manuscript, Available online 18 July 2018.

[19] Piergiuseppe Bettassa Copet, Guido Marchetto, Riccardo Sisto, and Luciana Costa. Formal verification of LTE-UMTS and LTE–LTE handover procedures. Computer Standards & Interfaces, Volume 50, Pages 92-106, February 2017.

[20] Divya Prerna, Rajkumar Tekchandani, and Neeraj Kumar. Device-to-device content caching techniques in 5G: A taxonomy, solutions, and challenges. Computer Communications, Volume 153, Pages 48-84, 1 March 2020.

[21] Pengcheng Wei, and Zhen Zhou. Research on security of information sharing in Internet of Things based on key algorithm. Future Generation Computer Systems, In press, accepted manuscript, Available online 12 May 2018.

[22] Qi Han, Yinghui Zhang, and Hui Li. Efficient and robust attribute-based encryption supporting access policy hiding in Internet of Things. Future Generation Computer Systems, Volume 83, Pages 269-277, June 2018.

[23] Jungyub Lee, Sungmin Oh, and Ju Wook Jang. A Work in Progress: Context based Encryption Scheme for Internet of Things. Procedia Computer Science, Volume 56, Pages 271-275, 2015.

[24] Sabrina Sicari, Alessandra Rizzardi, Daniele Miorandi, and Alberto Coen-Porisini. REATO: REActing TO Denial of Service attacks in the Internet of Things. Computer Networks, Volume 137, Pages 37-48, 4 June 2018.

[25] Xuanxia Yao, Zhi Chen, and Ye Tian. A lightweight attribute-based encryption scheme for the Internet of Things. Future Generation Computer Systems, Volume 49, Pages 104-112, August 2015.

[26] Abhijan Bhattacharyya, Tulika Bose, Soma Bandyopadhyay, Arijit Ukil, and Arpan Pal. LESS: Lightweight Establishment of Secure SessionA Cross-Layer Approach Using CoAP and DTLS-PSK Channel Encryption. 2015 29th International Conference on Advanced Information Networking and Applications Workshops, Pages 682-687, 2015.

[27] Kewei Sha, Wei Wei, T. Andrew Yang, Zhiwei Wang, and Weisong Shi. On security challenges and open issues in Internet of Things. Future Generation Computer Systems, Volume 83, Pages 326-337, June 2018.

[28] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, and Zied Chtourou. A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, Volume 4, Issue 2, Pages 118-137, April 2018.

[29] News. Securing the Internet of Things. Network Security, Volume 2018, Issue 1, Page 4, January 2018.

[30] Priyan Malarvizhi Kumar, and Usha Devi Gandhi. Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application. Springer, J Supercomput DOI 10.1007/s11227-017-2169-5, 2017.

[31] Roberto Morabito, Riccardo Petrolo, Valeria Loscrì, and Nathalie Mitton. Reprint of : LEGIoT: A Lightweight Edge Gateway for the Internet of Things. Future Generation Computer Systems, Volume 92, Pages 1157-1171, March 2019.

[32] Yuan Ai, Mugen Peng, and Kecheng Zhang. Edge computing technologies for Internet of Things: a primer. Digital Communications and Networks, Volume 4, Issue 2, April 2018, Pages 77-86.

[33] Bidyut Mukherjee, Songjie Wang, Wenyi Lu, Roshan Lal Neupane, Prasad Calyam. (2018). Flexible IoT security middleware for end-to-end cloud–fog communication. Future Generation Computer Systems, Vol. 87, pp. 688-703.

[34] Yan Sun, Fuhong Lin, Nan Zhang. (2018). A security mechanism based on evolutionary game in fog computing. Saudi Journal of Biological Sciences, Vol. 25, Issue 2, pp. 237-241.

[35] Jianbing Ni, Kuan Zhang, Xiaodong Lin. (2017). Securing Fog Computing for Internet of Things Applications: Challenges and Solutions. IEEE Communications Surveys & Tutorials, Vol. 20, Issue 1.

[36] Binara N. B. Ekanayake, Malka N. Halgamuge, Ali Syed. Review: Security and Privacy Issues of Fog Computing for the Internet of Things (IoT). Cognitive Computing for Big Data Systems over IoT, pp. 139-174.

[37] R. Rapuzzi, and M. Repetto. (2018). Building situational awareness for network threats in fog/edge computing: Emerging paradigms beyond the security perimeter model. Future Generation Computer Systems, Vol. 85, pp. 235-249.

[38] Cong Zuo, Jun Shao, Guiyi Wei, Mande Xie, and Min Ji. (2018). CCA-secure ABE with outsourced decryption for fog computing. Future Generation Computer Systems, Vol. 78, Part 2, pp. 730-738.

[39] Rodrigo Roman, Javier Lopez, and Masahiro Mambo. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. Future Generation Computer Systems, Vol. 78, Part 2, pp. 680-698.

[40] Ola Salman, Imad Elhajj, Ali Chehab, and Ayman Kayssi. (2018). IoT survey: An SDN and fog computing perspective. Computer Networks, Vol. 143, pp. 221-246.

[41] Alexandre Viejo, and David Sánchez. (2018). Secure and Privacy-Preserving Orchestration and Delivery of Fog-Enabled IoT Services. Ad Hoc Networks, In press, accepted manuscript, Available online 15 August 2018.

[42] Ismail Angri, Abdellah Najid, and Mohammed Mahfoudi. (2019). Available Bandwidth and RSRP Based Handover Algorithm for LTE/LTE-Advanced Networks Tested in LTE-Sim Simulator. International Journal of Electronics and Telecommunications, Vol. 65, No 1, pp. 85-93.

[43] Mohammed Mahfoudi, Moulhime El Bekkali, Abdellah Najd, M. El Ghazi, and Said Mazer. (2015). A New Downlink Scheduling Algorithm Proposed for Real Time Traffic in LTE System. International Journal of Electronics and Telecommunications, Vol. 61, No 4.

[44] Bujar Krasniqi, Blerim Rexha, and Betim Maloku. (2018). Energy Efficiency Optimization by Spectral Efficiency Maximization in 5G Networks. International Journal of Electronics and Telecommunications, Vol. 64, No 4, pp. 497–503.

[45] Faizan Qamar, MHD Nour Hindia, Talib Abbas, Kaharudin Bin Dimyati, and Iraj S. Amiri. (2019). Investigation of QoS Performance Evaluation over 5G Network for Indoor Environment at Millimeter Wave Bands. International Journal of Electronics and Telecommunications, Vol. 65, No 1, pp. 95-101.

[46] Muhammad Aziz ul Haq, and Sławomir Kozieł. (2017). Design Optimization and Trade-Offs of Miniaturized Wideband Antenna for Internet of Things Applications. Metrology and Measurement Systems, Vol. 24, No. 3, pp. 463–471.

[47] M. Głąbowski, S. Hanczewski, M. Stasiak, M. Weissenberg, P. Zwierzykowski, and V. Bai. (2020). Traffic Modeling in Industrial Ethernet Networks. International Journal of Electronics and Telecommunications, Vol. 66, No. 1, pp. 145-153.

[48] Xing Guo, Jinling Liang, and Jianquan Lu. (2021). Scaled consensus problem for multi-agent systems with semi-Markov switching topologies: A view from the probability. Journal of the Franklin Institute, Vol. 358, Issue 6, pp. 3150-3166

[49] Xihui Wu, and Xiaowu Mu. (2021). Practical scaled consensus for nonlinear multiagent systems with input time delay via a new distributed integral-type event-triggered scheme. Nonlinear Analysis: Hybrid Systems, Vol. 40, 100995.

[50] Bilal J. Karaki, and Magdi S. Mahmoud. Scaled consensus design for multiagent systems under DoS attacks and communication-delays. Journal of the Franklin Institute, Vol. 358, Issue 7, pp. 3901-3918.