Journal of Theoretical and Applied Information Technology
15th December 2020. Vol.98. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

OVERVIEW OF CHAMELEON MECHANISM IN B-MAC PROTOCOL FOR WSN

[1]ALAA K. Y.DAFHALLA, [2]NADA.M.O SID AHMED, [3] MOHAMED ELSHAIKH,[4]HIBA.M.ISAM

[1, 2] Department of Computer Engineering, College of Computer Science and Engineering, University of Ha'il, KSA

[3,4]Faculty of Electronic Engineering Technology, University Malaysia Perlis, Level 1, Pauh Putra Main Campus, 02600, Arau, Malaysia
E-mail: [1]loly.kam21@gmail.com, [2]nadamohamed11@gmail.com,
[3]elshaikh@unimap.edu.my,[4]heba,moh.1990@gmail.com

ABSTRACT

Wireless Sensor Networks (WSN) is gaining the interest of researchers due to numerous applications. WSN consists of sensor nodes connected with wireless technology to form a network. The sensor devices powered by the battery and collect the data from the environment and send to a base station. In the wireless sensor network, the topology changes frequently due to sensor nodes. The aforementioned behavior emphasis the impact of the MAC protocol mechanism in the performances of WSN. In recent years, the analysis of WSN MAC protocols and their impact on the performances of the network with different network scenarios has significantly developed a precise understanding of the requirements and goals for designing a MAC protocol. In the literature, many MAC protocol mechanisms are proposed to deal with WSN requirements. Nonetheless, proposed MAC mechanisms in the literature considered a single network scenario in WSN. However, the sensor nodes face some problems like the failure, addition, energy depletion, and movement which leads to different scenarios. The adhered behavior of WSN nodes results in a need for a MAC mechanism that addresses the requirement of more than one network scenarios. This paper, proposes a chameleon mechanism for MAC protocol to tackle topology changes in WSN. The proposed mechanism defines the performances of a MAC protocol in different network scenarios as a single and multiple objectives optimization problems. Further, a simulation implementation of the two methods above are presented. The discrete event simulator OMNET++5 and the INET3.5 modules are used for the simulation purposes in this work for their advantages in simulating wireless sensor network protocols and networks. The obtained results show that chameleon mechanism B-MAC reduce the power consumption of WSN for hybrid scenario.

Keywords: *B-MAC, Differential Evolution Algorithm, Power Consumption, Taguchi Method, WSN*

1. INTRODUCTION

Nowadays, wireless sensor network (WSN) provides solutions for different monitoring and control applications. These applications include environmental monitoring, target tracking, smart building, process monitoring, industrial automation, animal tracking system and healthcare application. WSN attracted the attention of researchers and development industries. The diversity of WSN applications, characteristics, and design requirements made researchers to continue looking for solutions, proposing new mechanisms, and protocols to solve issues related to WSN [1].

WSN contains sensor devices that embedded to perform a common task and send the collected data to a base station through wireless technology as illustrated in Figure 1. WSN provides services by deploying the sensor nodes in harsh environments, where sensor nodes to survive for extended periods of time [2].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

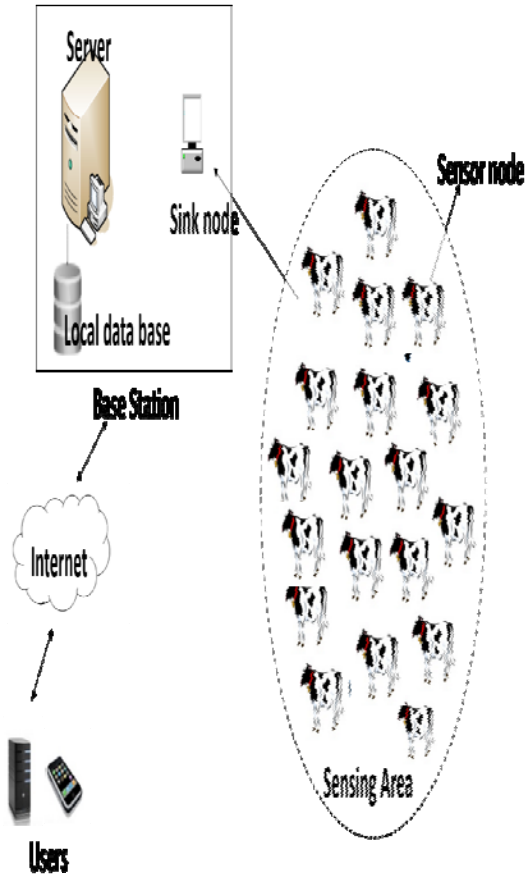

Figure 1: Example of WSN Architectures.

The main goal of sensor nodes (SNs) is to collect information from surrounding environment and send it to a base station (BS). BS has a large memory, and storage system for data storage. Moreover, the BS performs additional functions such as data analysis and visualizations, graphical user interface to interact with the user, data forwarding to remote server via the internet, and handling of sensor network routing or node configuration [3]. The rest of the paper is organized as follow: Section two highlights some previous work in the same direction of this paper. Section three gives an overview of the chameleon mechanism and description of the proposed work. Section four reviews and discusses the obtained results of this work. Finally, the work in this paper is concluded in the last section.

2. RELATED WORK

CM was introduced by (Krawczyk & Robin, 1998) as a hashing mechanism used in data cryptographic. Since its introduction, the CM has been used in many works to mimic chameleon lizard behavior with different concepts.

K.Cheng et al (2019) The Controller Area Network (CAN) has been widely used in the automotive and industrial automation for over two decades. However, due to the lack of security mechanisms, CAN is vulnerable to attacks. proposed a novel protection scheme called CANeleon. It can defend CAN against a smart attacker who might inject malicious frames with the legitimate frame IDs, which cannot be mitigated by existing countermeasures. Inspired by the idea of moving target defense technologies, CANeleon equips each legitimate CAN node with the ability to shift the spoofed frame ID. In this way, the ID of malicious frames is exposed and can be further filtered by legitimate nodes. Moreover, CANeleon neither inserts new information to the frame, nor requires any modification to the CAN protocol, so it is in compliance with the existing standards. CANeleon is a decentralized mechanism guaranteeing that the protection could be done simultaneously without additional communication. Experiments on a CAN bus prototype and a real self-driving vehicle proved the effectiveness of CANeleon [4].

Kartit.Z & Diouri. (2019) recent years, individuals and organizations have been using digital services created by digital transformation. With smart mobile devices, there is a lot of enthusiasm for providing users with the ability to shop, communicate, and access to information anytime and from anywhere. The Ad hoc mobile network (MANET) as an important wireless technology can be used to exploit these services. In consideration of the sensitivity of users' data routed through network nodes, secure routing must be the priority of MANET networks. Due to their characteristics such as a dynamic topology, a distributed control system, limited resources and multi-hop communication, these networks are particularly vulnerable to different security threats [5].

Iyer, Worehrle, and Langendoen (2010) CM used to overcome external interference problems. The chameleon mechanism is hosted on the network and external hosts that shared the same spectrum. CM is divided into two distinct parts: firstly, a switch mechanism that devises the control logic of changing channels when it is necessary. Secondly, a switch policy that specifies the conditions on which to perform a switch [6].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Leone, Papatriantafilou, Schiller, and Zhu (2010) adapts the Chameleon-MAC in mobile ad hoc network (MANET). The concept of the chameleon-MAC algorithm; in self-stabilizing MAC algorithm, takes the scheduled approach and adapts to the variable environment of MANET. CM algorithm adapts to a variable environment in which relocation parameters, as well as the size of the interference neighborhoods, can change [7].

j and Xia, (2016) used CM to improve the near field communication (NFC) service. NFC is a new technological development for contactless devices. Further, NFC enables smartphones and other supported devices to communicate with other devices containing an NFC tag. The communication between two NFC devices can perform the identity verification, payment services, and information sharing. The main problem faced by NFC is relay attacks; such as malicious link via relay channel to force payment transactions or steal valuable financial information. However, to avoid this problem CM plays a vital role, by exchanging the roles of the two NFC devices after every NFC session, in a random manner, which is unpredictable by the hacker. CM can detect if the device in the vicinity is legal, thereby improves the performance, and provide more security [8].

3. METHODOLOGY

The paper aims to reduce the power consumption of WSN implementation by using mechanism called Chameleon mechanism – Berkeley MAC. Chameleon mechanism (CM) is proposed to adapt to different topology network by adjusting the parameters of a MAC protocol to the current topology requirements. Moreover, CM uses optimization process to determine optimum values (OVs) of the B-MAC protocol for a target network scenarios partial farms (PF1 and PF2). Optimization process in CM accomplished based on the following two optimization techniques: firstly, Taguchi method (TM) for single objective as mentioned in [9] and secondly, differential evolution algorithm (DEA) for multi- objective [10] as depicts in Figure 2.

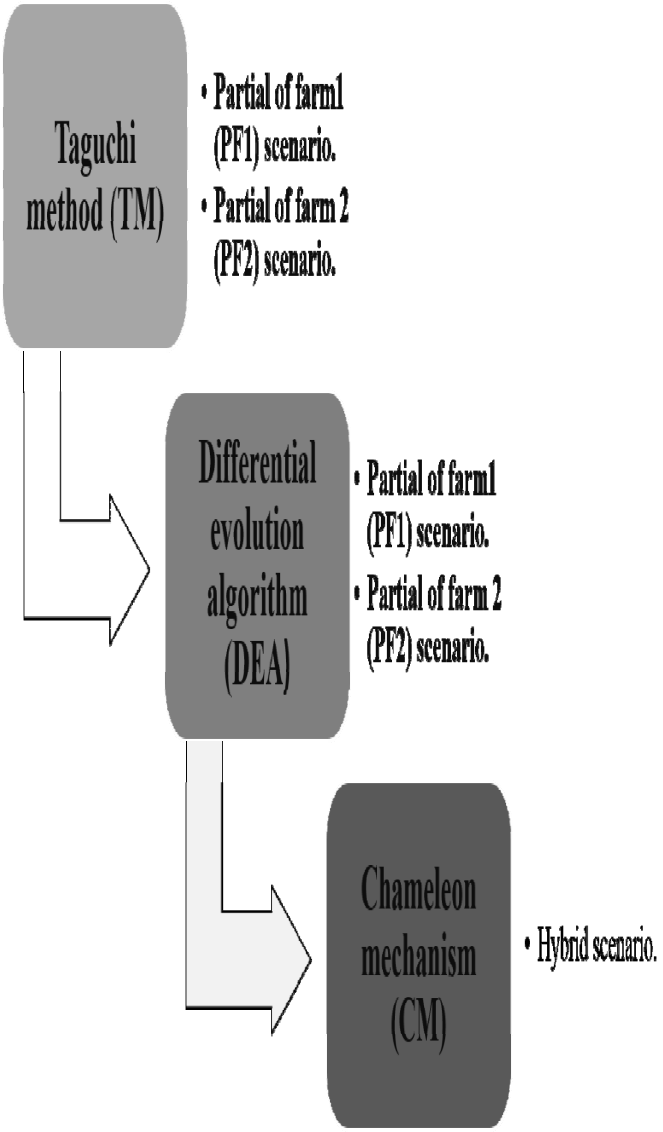

Figure 2: Optimization Phases of the Chameleon Mechanism.

The B-MAC optimization process was accomplished by using two optimization methods: Taguchi method (TM) and differential evolution algorithm (DEA). The optimization process was started by optimizing the B-MAC parameters protocol for a particular scenario and performance metrics [11]. The main goal of optimization processes is to find optimum values (OVs) of the B-MAC parameters. TM process is used to identify the best solutions for parameters B-MAC that optimizes the following network performance metrics; power consumption, throughput, PDR, and delay. In addition, optimum solution obtained by TM is used as initial conditions for DEA to find a single solution for all network performance metrics.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The two stages optimization process results in a set of parameters values of a B-MAC protocol in each WSN scenarios as illustrated in Figure 3. Moreover, the optimization results are used to design and implements CM.

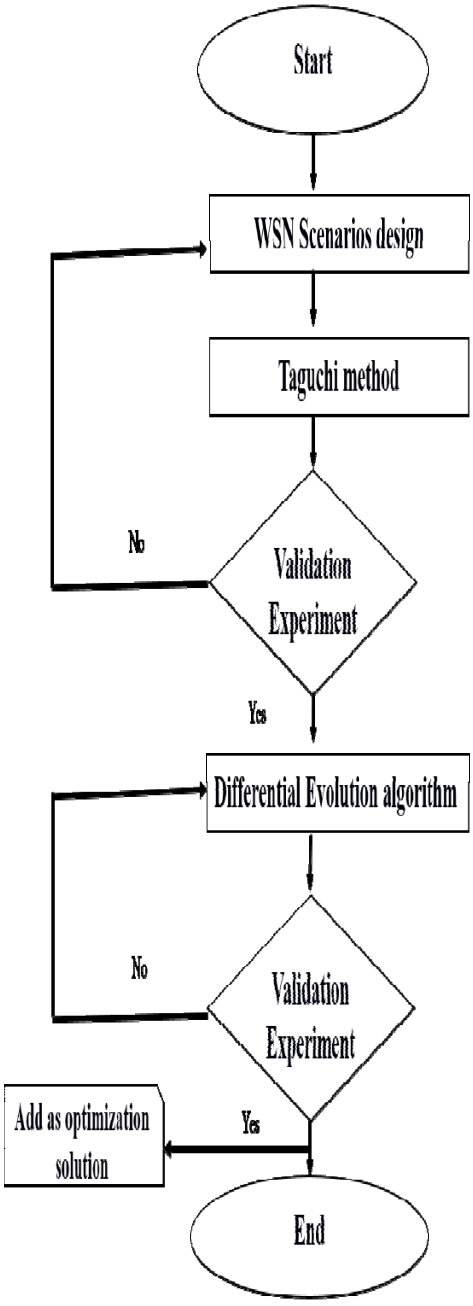

Figure 3: The Optimization Phases Flowchart.

3.1 Chameleon Mechanism Design and implementation

Chameleon Mechanism (CM) is inspired by the chameleon lizard that has an ability to adjust its skin color within an environment. Similarly, the CM is aimed at adjusting the parameters of a B-MAC protocol. CM increases the energy-saving opportunities for the multi-configuration WSN network.

This phase concentrates on the design of the CM and its integration with B-MAC protocol. CM is aimed at reducing power consumption of MAC protocol in multi-configuration for WSN when sensor nodes move from one network scenario to another. Furthermore, the obtained optimum solutions are integrated with the MAC protocol as Merge Taguchi Differential Evolution (MTDE) profile to the desired WSN scenario. Then, B-MAC protocol is selected as the best profile for the current running situation. Figure 4 shows the flowchart of the CM. If determines a new scenario CM apply MTDE profile, else CM apply the default values. CM assumed that the best solution is given for each WSN scenario, which is obtained in the optimization phase. B-MAC protocol is selected to integrate the CM for power consumption merits as follow:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

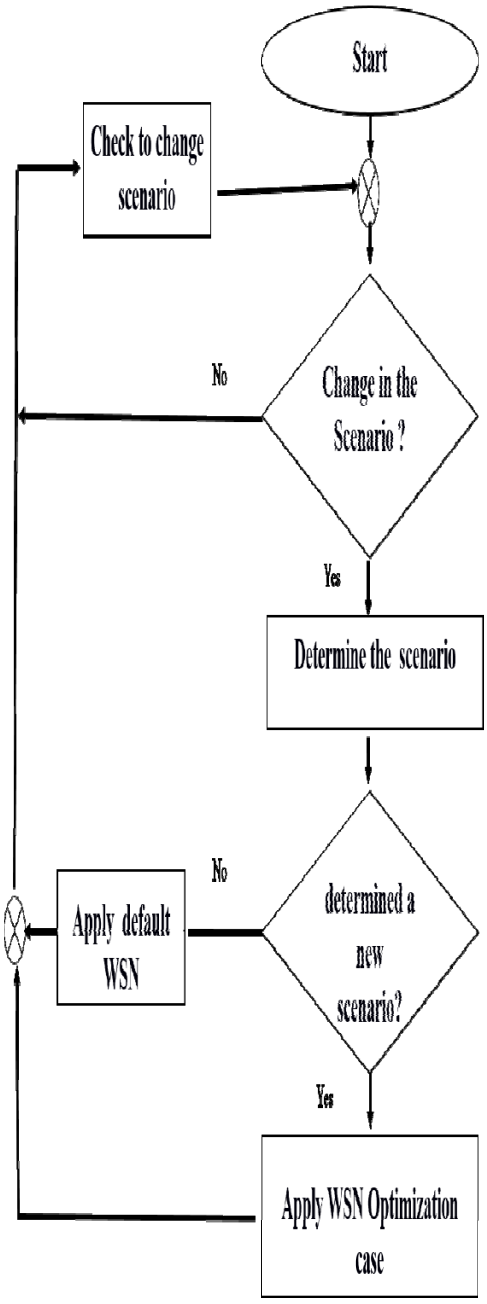

Figure 4: Chameleon Mechanism Flowchart.

3.2 Chameleon Mechanism MAC Protocol (CM-MAC)

CM-MAC is inspired by the chameleon lizard that could adjust the skin color within an environment. CM-MAC mechanism provides a MAC protocol configuration an ability to adapt to a specific scenario and network requirements.
CM combines the optimization process with request/reply (REQ/REP) mechanism for B-MAC protocol. Further, the difference between CM-BMAC and previous chameleon methods is MTDE control message (MCM) uses to perform optimization process. Optimization methods achieve optimum values (OVs) for a specific network scenario and save it as Merge Taguchi Differential Evolution (MTDE) profile in the base station (BS). REQ/REP mechanism added to the sensor nodes (SNs) for adopting the MTDE profile based on the current specific network as illustrated in Figure 5.

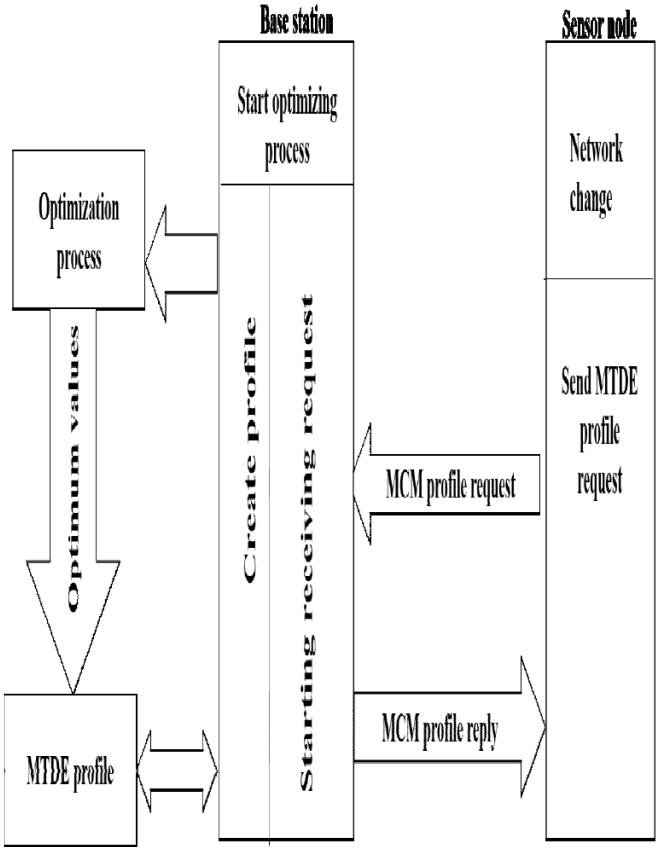

Figure 5: Chameleon Mechanism MAC Process.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In CM-MAC, BS performs the optimization process to find OVs and saves it as MTDE profile. Then, SN selects the nearest BS defined as target BS. The nearest BS is chosen based-on distance. Moreover, SNs obtain optimized configuration profile from their target BS by sending a profile request message. BS replies to the profile request message with the update profile saved**.**

3.2.1 Optimization Mechanism Implementation

Optimization methods (TM and DEA) are implemented for B-MAC protocol. The goal of this method is to find OVs for a running WSN scenario and define it as MTDE profile. Further, the main goal of MTDE profile is to save OVs, to reduce the power consumption without an effect on network performance. MTDE profile is executed by performing TM and DEA as described in [9] [10].

DEA method uses the fitness function (FF) to find the optimum solution. FF reflects the relation between the B-MAC parameters and optimization target. The implementation of FF in a MAC protocol is performed by choosing k experiments from Taguchi orthogonal array (TOA) and broadcasting a control message in the network. Then, measures the network performances for the received responses. These operation results, are measuring the performances of the network for different configurations online with TOA design of experiments and store it in a result table. By repeating the last process for N times, the mechanism will be able to perform the DEA calculations [4] and obtains the DEA to find one solution for all network performances.

The optimization process divides the network nodes into the BS and SNs. BS are responsible for initiating the optimization process and save the optimum solution as MTDE profile. SN response to the BS message with a formatted reply message. The communication between SNs and BS are performed with the use of a specially designed message named MTDE control Message (MCM). The structure of MCM is shown in Figure 6. MCM are three types: MCM, REP, and MTDE profile.

1) MCM: MCM is used for broadcasting the optimization desired configuration; when the BS begins the optimization process. MCM type data carries values for four parameters that represent the control factors (CFs) values for one experiment in the TOA. MCM –id is a unique incremental sequence number generated by the BS to identify the optimization operation. MCM- k is the number of an experiment in the TOA for the message. MCM- id and MCM- k are created by the BS and are used by the SN, to identify the process and experiment number of the received message.

2) REP: REP type has the same header as MCM, but carries different data. REP data contains the SN IP Address and the decision made for its target BS. REP is generated by SN and sent in unicast to a specific BS. REP is exploited by the BS to calculate the FF for the kth experiment in the TOA, where k is the MCM- k field in the header.

3) MTDE Profile: this type is generated by the BS at the end of the optimization process. MTDE Profile type carried OVs configuration for the network, and send to sensor nodes within the range of the base station. The MCM- id is used by sensor node to identify the up-to-date of the carried configuration. Other parameters in the header are ignored for this type.

The process of optimization is divided into two parts: SNs and the BS. The following subsection detailed these processes for each part:

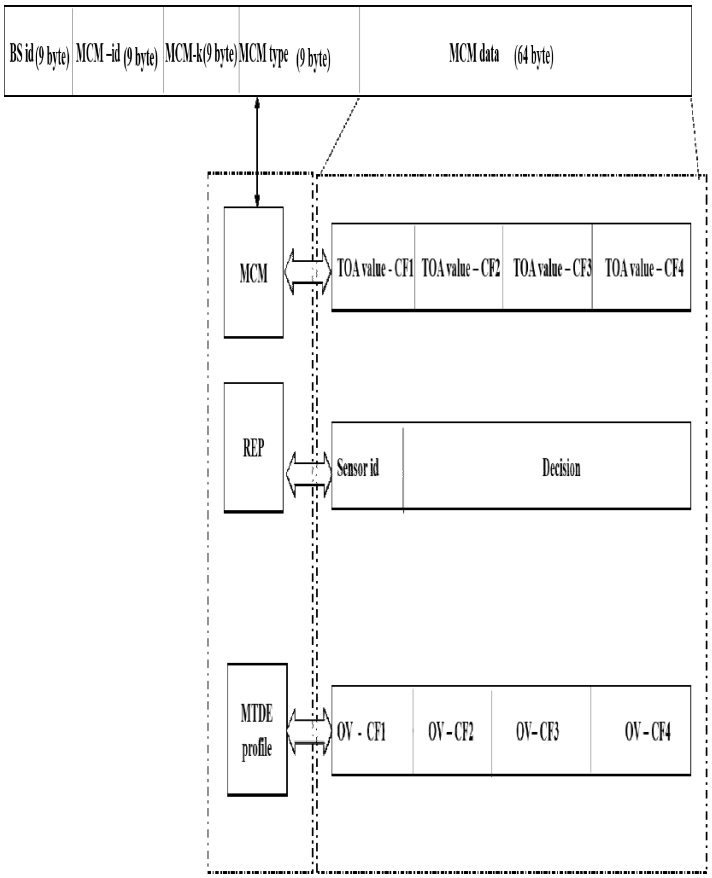

Figure 6: MTDE Control Message (MCM) Structure.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Sensor node (SN) receives two types of requests from the BS: MCM and MTDE profile. MCM type is received during the broadcast operation, and MTDE profile type is received at the end of the operation. Moreover, when the SN receives MCM it starts evaluating the MCM configuration and then generates a REP –MCM message. REP-MCM contains two types of information: sensor- id and decision. Furthermore, sensor- id is the IP address of the sensor node, and the second parameter is a decision made based on information contained on the MCM to target BS. For the SNs to make the decision, it starts by evaluating the configurations in the MCM. Furthermore, the MCM configuration contains the slot duration, bit rate, check interval, and Tx power. The evaluation process is accomplished by comparing their values in the MCM message and the current configuration in the protocol**.**

The base station (BS) performs several tasks, beginning from the start the optimization process, broadcast to SNs, creates the MTDE profile by defining OVs, and receiving the MCM profile request. The time process following these operations is presented in Figure 7.

The optimization process is achieved in the BS and puts into consideration any changes in the network scenario. Further, the controlled optimization process is accomplished by network administration.

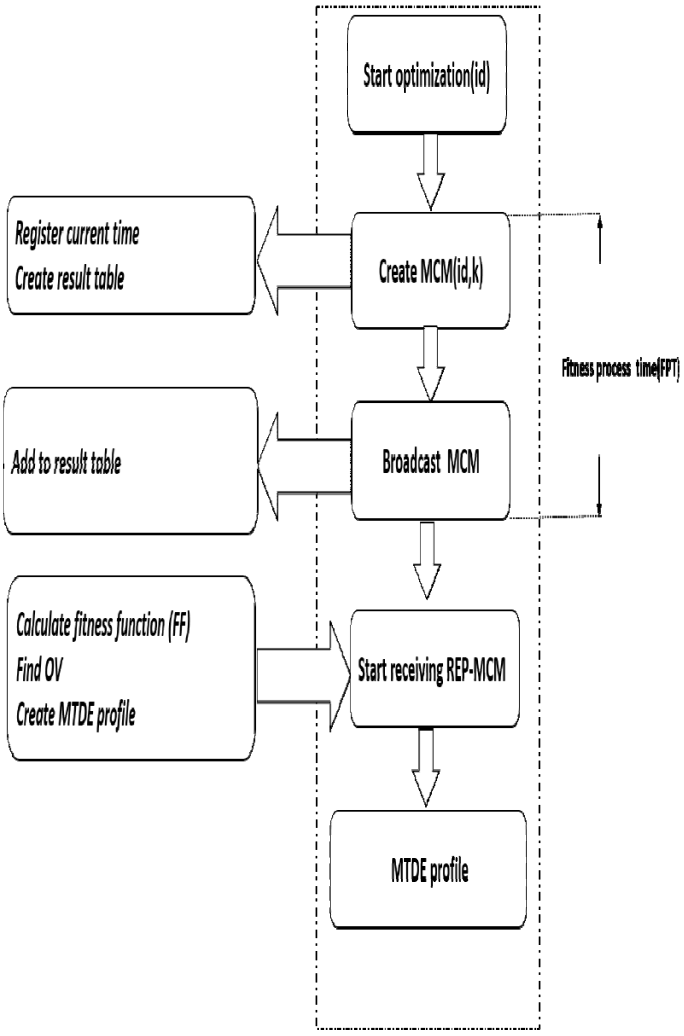

Figure 7: The Optimization Implementation Process in the Base Station (BS).

Optimized process achieved by two methods TM and DEA. Firstly, TM is used to determine the control factors, Taguchi orthogonal array (TOA), and signal to noise (S/N) analysis [3].

DEA process begins by evaluating fitness function (FF) coefficients for the running scenario described in Equation 1 [4].

$FF(x_1, x_2, x_3, x_4)$ = f [power consumption, PDR, throughput, delay] (1)

x_1, x_2, x_3, and x_4 refer to control factors (CFs) of B-MAC protocol and the goal of DEA is to optimize f.

FF coefficients are calculated by substituting four set of experiments from the results array in Equation 2.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$Ax_1+Bx_2+Cx_3+Dx_4$=[delay+1/throughput]×1/PDR× power consumption (2)

The optimization process at the BS starts by generating a set of the MCM message and creating a results table. The generated message is broadcasted to the network and the BS starts the receive REP-MCM mode. BS in the receive REP-MCM mode accepts and process the incoming REP-MCM to update the result table with statistics for performing FF. The optimization calculation generates MTDE profile with the use of TM and DEA methods. The flowchart explains this operation is illustrated in Figure 8. The implementation of the method mentioned above is adopted to B-MAC protocol. The resulted configuration profiles are then used by the chameleon mechanism to complete the process of the CM-BMAC protocol.

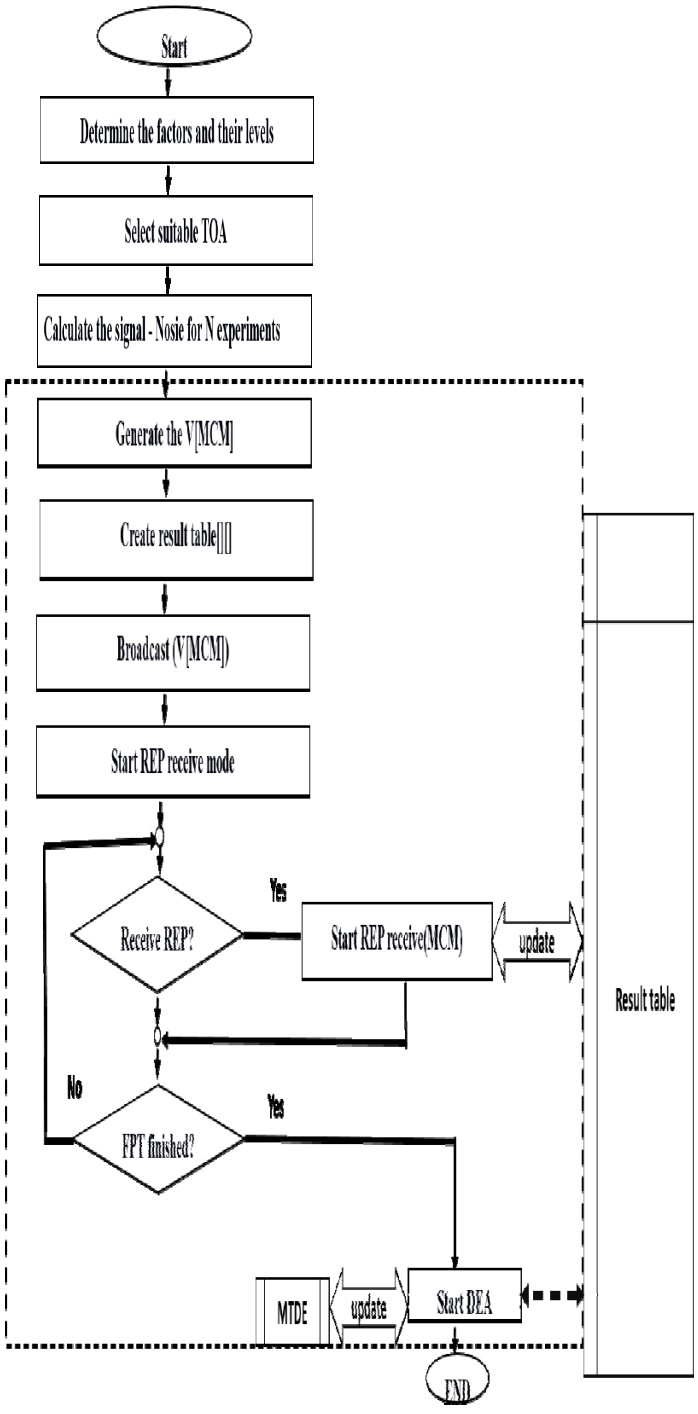

Figure 8: Optimization Implementation on BS

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. Results

This Section presents a comparison between CM-BMAC, B-MAC, and IEEE802.15.4 performances against the different number of nodes. Power consumption is utilized to evaluate the effects of the different number of nodes in the network power consumption. The comparisons are performed in the hybrid scenario mentioned in Table 1. Further, the number of nodes are explained in Table 2.

Table 1: The simulation parameters of WSN scenarios.

Parameters	PF1	PF2	Hybrid
Dimension	200m x 400m	200m x 400m	400m x 400m
Node speed	1-4 Km/h	0	1-4 Km/h
Number of nodes	43 sensor nodes	16 cameras	59
Transmission range	100m	100m	100m
Number of base station	3	3	6
MAC protocol	B-MAC	B-MAC	B-MAC
Traffic generation model	Burst application	Burst application	Burst application
Packet size	512 byte	1024 byte	1024 byte

Table 2: Number of nodes in hybrid scenario.

Experiment NO	1	2	3	4	5	6
Number of nodes	10	20	30	40	50	59

Figure 9 shows the observed power consumption for CM-BMAC, B-MAC, and IEEE802.15.4 for a different number of nodes. Denoted the power consumption is proportional to the number of nodes. Further, at the 59 nodes because hybrid scenario combine between PF1 and PF2 scenarios; CM-BMAC increases the power consumption to 15.8mW, B-MAC provides 20.85mW, and IEEE802.15.4 gives the power consumption about 30.23mW. The observed results concluded the impact of optimization on the efficiency of a B-MAC protocol. Moreover, it is has shown the influences of B-MAC parameter in reducing power consumption. Furthermore, coefficient of variation is 19.35%, 24.56%, and 26.36% for CM-BMAC, B-MAC, and IEEE802.15.4 respectively. So it is quite evident that the dispersion is lower in the CM-MAC than the B-MAC and IEEE802.15.4.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

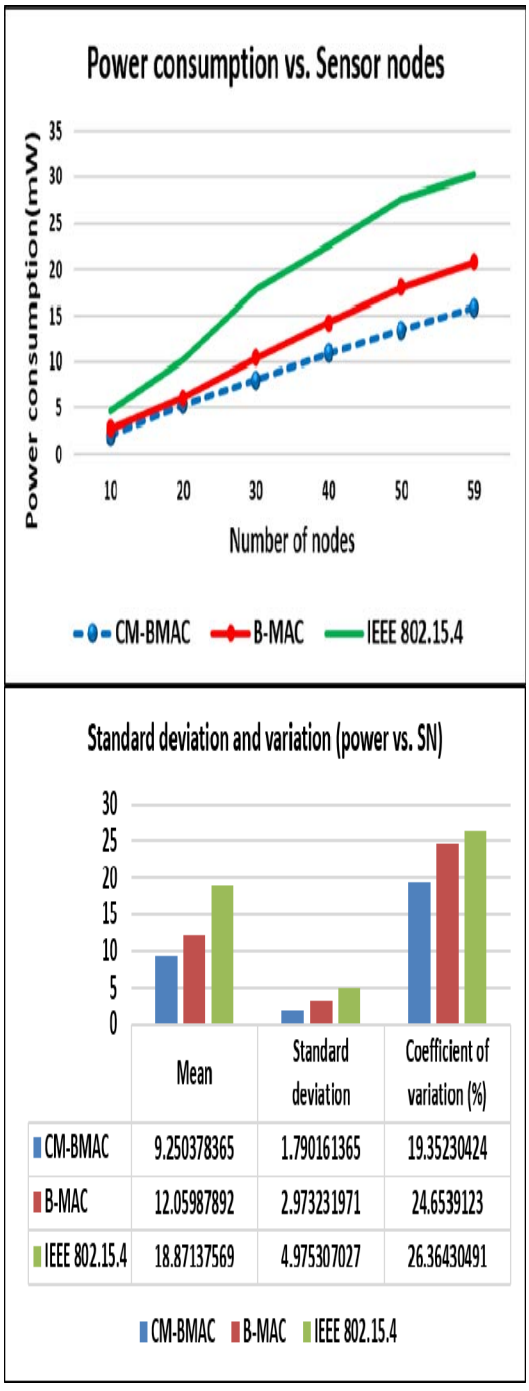

Figure 9: Power and Standard Deviation Consumption Comparison between CM-BMAC, B-MAC, and IEEE802.15.4 for Different Number of Nodes

4. CONCLUSION

Chameleon mechanism CM-BMAC aims to improve the successor B-MAC with topology changes in WSN. Consequently, the power consumption is evaluated and compared to B-MAC in different WSN scenarios and compared to IEEE802.14.5 as well. The performance evaluations of CM-BMAC is performed in hybrid WSN scenario. OMNET++5 and INET3.5 simulation tools are used for the experiments in this paper. The obtained results showed that CM-BMAC outperformed B-MAC regarding power consumption, in the simulated WSN scenario. Further, CM-BMAC improved the robustness by maintaining higher performances in different WSN scenarios and the hybrid scenario. CM mechanism considered the scenario from a number of nodes. However, network scenarios can be reflected by different network requirements aspects including network type, application requirements, and scalability. Hence, the integration of this mechanism by considering mobility, application requirements, scalability, and security can provide new directions for the future works of the CM mechanism.

REFRENCES:

[1] T. Dao, J. Yu, T. Nguyen and T. Ngo, "A Hybrid Improved MVO and FNN for Identifying Collected Data Failure in Cluster Heads in WSN," *in IEEE Access*, vol. 8, pp. 124311-124322, 2020.

[2] Fotohi, R., Firoozi Bari, S. A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms. *J Supercomput 76*, 6860–6886 2020.

[3] J. Uthayakumar, M. Elhoseny and K. Shankar, "Highly Reliable and Low-Complexity Image Compression Scheme Using Neighborhood Correlation Sequence Algorithm in WSN," *in IEEE Transactions on Reliability*, doi: 10.1109/TR.2020.2972567.

[4] K. Cheng, Y. Bai, Y. Zhou, Y. Tang, D. Sanan and Y. Liu, "CANeleon: Protecting CAN Bus with Frame ID Chameleon," *in IEEE Transactions on Vehicular Technology*,2019, doi: 10.1109/TVT.2020.2990417.

[5] Kartit.Z & Diouri. "Security Extension for Routing Protocols in Ad hoc Mobile Networks: A comparative Study" NISS19: *Proceedings of the 2nd International*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Conference on Networking, Information Systems & Security, March 2019 Article No.: 69 Pages 1–7.

[6] Iyer, V., Woehrle, M., & Langendoen, K. (2010). Chamaeleon – exploiting multiple channels to mitigate interference. *2010 Seventh International Conference on Networked Sensing Systems (INSS)*, 65-68.

[7] Leone, P., Papatriantafilou, M., Schiller, E. M., & Zhu, G. (2010). Chameleon-MAC: Adaptive and self- algorithms for media access control in mobile ad hoc networks. *Lecture Notes in Computer Science*, 6366, 468–488.

[8] Ji, Y., & Xia, L. (2016). Improved chameleon: A lightweight method for identity verification in near field communication. *2016 International Symposium on Computer*, Consumer and Control (IS3C), 387-392.

[9] Kamal.A, Warip.M.N, ELSHAIKH.M, & .BADLISHAH. R. (2017). Power consumption Optimization based on B-MAC protocol for multi-scenario WSN by Taguchi method. *Lecture Notes in Data Engineering and Communication Technologies*, 2017.

[10] Kamal.A, Warip.M.N, ELSHAIKH.M, & .BADLISHAH. R. (2017). Optimization of B-MAC protocol for multi- scenario WSN by differential evolution algorithm. *Lecture Notes in Data Engineering and Communication Technologies*, 2017.

[11] Kamal.A, Warip.M.N, & ELSHAIKH.M. (2017). THE IMPACT OF INNER-PARAMETERS B-MAC PROTOCOL BY TAGUCHI METHOD FOR WSN. vol. 98, no. 05, pp. 788–797, 2020.