Mohamed Elhoseny · Amit Kumar Singh
Editors

Smart Network Inspired Paradigm and Approaches in IoT Applications

Springer

Smart Network Inspired Paradigm and Approaches in IoT Applications

Mohamed Elhoseny · Amit Kumar Singh
Editors

Smart Network Inspired Paradigm and Approaches in IoT Applications

Springer

Editors
Mohamed Elhoseny
Faculty of Computers and Information
Mansoura University
Mansoura, Egypt

Amit Kumar Singh
Department of Computer Science
and Engineering
National Institute of Technology Patna
Patna, India

ISBN 978-981-13-8613-8 ISBN 978-981-13-8614-5 (eBook)
https://doi.org/10.1007/978-981-13-8614-5

© Springer Nature Singapore Pte Ltd. 2019
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

Smart networks' architectures and technologies play an important and increasing role in practice due to the widespread adoption of mobile devices in many applications. For example, from the industry perspective, the synergy between smart mobile networks and cloud technologies has resulted in new cloud provisioning models for supporting mobile application development and deployment. From an academic perspective, smart networks are a way of augmenting mobile devices and dealing with the inherent limitations related to remote resources located in IoT applications. Techniques materializing this idea include off-loading and cyber foraging. While smart networks can be viewed as a special case of ad hoc and sensors networks, it represents also an evolution of the latter since it includes the ability of augmenting mobile (e.g., laptops, smartphones, tablets, and wearables) and wireless devices (e.g., sensors and actuators) with processing/storage resources in their proximity, in terms of network topology. Indeed, several flavors of this idea, including micro-data centers, cloudlets, and fog computing itself, follow the edge computing model, by which data/computations are processed using computing resources located at the edge of the network—accessible through wireless protocols—and optionally using remote resources in the cloud.

Motivated not only by the increasing number of mobile devices, but also by their ever-growing computing and sensing capabilities, there have been efforts to leverage these devices as a destination for off-loading computations/data in the context of IoT applications. Such a trend has also been referred to as dew computing in the literature. However, current research in the area is still focused on augmenting mobile clients via fixed computing resources (e.g., local servers and computer clusters), so huge unexploited computing and sensing capabilities remain "at the edge." Therefore, many research opportunities to exploit mobile devices in the context of smart networks for IoT applications arise.

In view of the above, this book presents the state-of-the-art techniques and approaches, design, development, and innovative use of smart networks' inspired paradigm and approaches in IoT as well as other demanding applications. Various recent algorithms and novel/improved techniques are discussed in this book.

The authors believe that this book would provide a sound platform for understanding the smart networks' inspired paradigm and approaches/issues in emerging applications, prove as a catalyst for researchers in the field, and shall be equally beneficial for professionals. In addition, this book is also helpful for the senior undergraduate and graduate students, researchers, and industry professionals working in the area as well as other emerging applications demanding smart networks.

We are sincerely thankful to all the authors, editors, and publishers whose works have been cited directly/indirectly in this manuscript.

Special Acknowledgements

The first editor gratefully acknowledges the authorities of *Mansoura University, Egypt*, for their kind support to complete this book.

The second editor gratefully acknowledges the authorities of *National Institute of Technology Patna, India*, for their kind support to come up with this book.

Mansoura, Egypt — Dr. Mohamed Elhoseny
Patna, India — Dr. Amit Kumar Singh

Contents

A Reactive Hybrid Metaheuristic Energy-Efficient Algorithm for Wireless Sensor Networks 1
N. Shivaraman and S. Mohan

Maintaining Consistent Firewalls and Flows (CFF) in Software-Defined Networks 15
A. Banerjee and D. M. Akbar Hussain

Energy-Efficient Broadcasting of Route-Request Packets (E^2BR^2) in Ad Hoc Networks 25
Anuradha Banerjee and Subhankar Shosh

Decision Support System for Smart Grid Using Demand Forecasting Models 47
Sonali N. Kulkarni and Prashant Shingare

Internet of Things—The Concept, Inherent Security Challenges and Recommended Solutions 63
Burhan Ul Islam Khan, Rashidah F. Olanrewaju, Farhat Anwar, Roohie Naaz Mir, Allama Oussama and Ahmad Zamani Bin Jusoh

Critical Challenges in Access Management Schemes for Smartphones: An Appraisal 87
Tehseen Mehraj, Burhan Ul Islam Khan, Rashidah F. Olanrewaju, Farhat Anwar and Ahmad Zamani Bin Jusoh

Using Fuzzy Neural Networks Regularized to Support Software for Predicting Autism in Adolescents on Mobile Devices 115
Paulo Vitor de Campos Souza, Augusto Junio Guimaraes, Vanessa Souza Araujo, Thiago Silva Rezende and Vinicius Jonathan Silva Araujo

Performance Evaluation of Supervised Machine Learning Classifiers for Analyzing Agricultural Big Data 135
R. Anusuya and S. Krishnaveni

WordNet Ontology-Based Web Page Personalization Using Weighted Clustering and OFFO Algorithm 151
N. Balakumar and A. Vaishnavi

Mobility Condition to Study Performance of MANET Routing Protocols 169
Hind Ziani, Nourddine Enneya, Jihane Alami Chentoufi and Jalal Laassiri

Security Requirements and Model for Mobile Agent Authentication 179
Sanae Hanaoui, Jalal Laassiri and Yousra Berguig

Internet of Thing for Smart Home System Using Web Services and Android Application 191
Khaoula Karimi and Salahddine Krit

Bat with Teaching and Learning Based Optimization Algorithm for Node Localization in Mobile Wireless Sensor Networks 203
G. Kadiravan and Pothula Sujatha

A Next Generation Hybrid Scheme Mobile Graphical Authenticator 221
Teoh Joo Fong, Azween Abdullah and Hamid Reza Boveiri

Energy Efficient MANET by Trusted Node Identification Using IHSO Optimization 239
S. Krishnaveni and N. Angel

About the Editors

Dr. Mohamed Elhoseny is currently an Assistant Professor at the Faculty of Computers and Information, Mansoura University, Egypt, where he is also Director of the Distributed Sensing and Intelligent Systems Lab. Dr. Elhoseny has authored or co-authored over 100 ISI journal articles, conference proceedings, book chapters, and several books published by Springer and Taylor & Francis. His research interests include Network Security, Cryptography, Machine Learning Techniques, and Intelligent Systems. Dr. Elhoseny serves as the Editor-in-Chief of the International Journal of Smart Sensor Technologies and Applications, and as an Associate Editor of several journals such as IEEE Access.

Amit Kumar Singh received the bachelor's degree and M.Tech. in computer science and engineering from Veer Bahadur Singh Purvanchal University, Jaunpur, India (2005) and Jaypee University of Information Technology, Waknaghat, India (2010), prior to completing his Ph.D. degree in computer engineering at the National Institute of Technology, Kurukshetra, India (2015). He worked at the Computer Science and Engineering Department, Jaypee University of Information Technology, from 2008 to 2018. He is currently an Assistant Professor at the Computer Science and Engineering Department, National Institute of Technology at Patna (An Institute of National Importance), Patna, India. Dr. Singh has authored over 80 peer-reviewed journal articles, conference publications, and book chapters, as well as the books Medical Image Watermarking: Techniques and Applications (2017), and Animal Biometrics: Techniques and Applications (2018, Springer International Publishing). He has also edited several books and currently serves on the Editorial Board of two peer-reviewed international journals. His research interests include Data Hiding, Biometrics, and Cryptography.

A Reactive Hybrid Metaheuristic Energy-Efficient Algorithm for Wireless Sensor Networks

N. Shivaraman and S. Mohan

Abstract Expanding network lifespan is the main target during the design of a wireless sensor network. Clustering the sensor nodes is an efficient topology to accomplish this objective. In this work, we offer a reactive hybrid protocol to enhance network lifetime using the hybridization of ant colony optimization (ACO) along with particle swarm optimization (PSO) algorithm. In order to improve the energy efficiency, the anticipated RAP algorithm uses a reactive data transmission strategy which is incorporated into the hybridization of ACO and PSO algorithm. In the beginning, the clusters are organized depending on the residual energy and then the proposed RAP algorithm will be executed to improvise the inter-cluster data aggregation and reduces the data transmission. The experimental outcomes demonstrate the proposed RAP algorithm performs well against other near conventions in different situations.

Keywords WSN · Clustering · Energy efficiency · ACO · PSO

1 Introduction

A wireless sensor network (WSN) is an autonomous wireless network framework comprising of various sensors, which assemble data from their encompassing surroundings as well as broadcast it to an information sink or a base station (BS) [1]. In WSN applications, the primary target is to screen and gather sensor information as well as afterward broadcast information to the BS. Sensors in various areas of the field are able to work together in information accumulation, in addition, to give better precise reports over their neighborhood areas. Mostly, WSNs measures the physical phenomena such as temperature, pressure, acoustic, or area of objects [2], to enhance

N. Shivaraman (✉)
Department of Computer and Information Science, Annamalai University, Chidambaram, India
e-mail: ramansiva28@gmail.com

S. Mohan
Department of Computer Science and Engineering, Annamalai University, Chidambaram, India
e-mail: mohancseau@gmail.com

© Springer Nature Singapore Pte Ltd. 2019

M. Elhoseny and A. K. Singh (eds.), *Smart Network Inspired Paradigm and Approaches in IoT Applications*, https://doi.org/10.1007/978-981-13-8614-5_1

the accuracy of detailed estimations, as well as information collection decreases the communication congestion in the network, prompting huge energy saving [3–6]. The qualities of minimal effort, low-control, as well as multifunctional sensors have rendered WSNs extremely appealing in different dimensions [7, 8]. These days, with the improvement of cloud innovation [9], WSNs quickly conveyed numerous viable applications, comprising home security, battle-zone reconnaissance, observing the development of undomesticated creatures in the forest, healthcare applications [10, 11], and so forth [12]. Within a sensor network, every node can be a sensor as well as a router. In addition to its computing capability, storage capacity, as well as communication ability, are also the constraints of WSN [13–15]. In addition, in numerous WSN applications, sensor nodes are dispensed into a harsh condition, that makes the substitution of failed nodes moreover troublesome otherwise costly [16–18]. In this way, in numerous situations, a wireless node has to work without battery recharging for an expanded time frame [19]. Thus, energy efficiency is the major issue while planning a WSN by means of the goal of improved network lifespan [7, 20, 21]. Energy utilization might be able to be effectively overseen via modifying the network topology as well as managing the nodes' transmission control in the routing convention [22, 23].

The clustering method is helpful in diminishing the amount of data transmission as well as save energy consumption [24]. Within a clustering design, sensor nodes be formed into clusters, wherever the sensor nodes by means of bring down energy may be able to be utilized to carry out detecting undertakings, and send the detected information to their cluster head (CH) in the nearby distance [25–28]. The clustering model is shown in Fig. 1. A node inside a cluster might be able to be selected as CH to collect the information out of the member of the cluster, through the target of decreasing the transmission distance of the accumulated information transferred to the BS [29, 30].

The clustering method can build network longevity as well as enhance energy proficiency by limiting energy utilization as well as adjusting energy utilization among the nodes [31, 32]. Also, it is equipped for minimizing channel contention

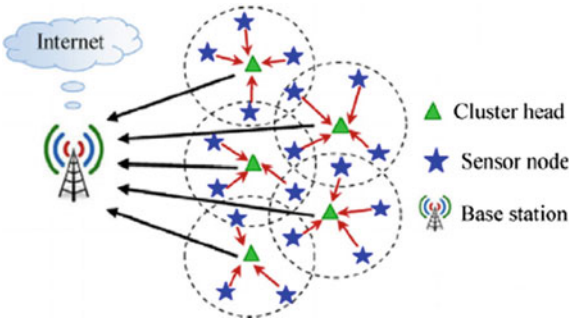

Fig. 1 Clustering architecture

as well as packet collisions, bringing about enhanced network throughput beneath high load [33, 34]. In a standard point of view, the process of optimization can be described to find the best solution of the function from the system within constraints [35–38]. The principal objective of the swarm and evolutionary algorithms (EA) depends on clustering conventions to powerfully cluster sensor nodes in the setup stage so the energy utilization is limited as well as clustering criteria be improved. For N sensor nodes, here are absolutely 2^{N-1} distinctive arrangements, wherever in every arrangement, every node may be able to be whichever chosen as a CH or not. Accordingly, clustering within WSNs is an NP-hard issue. EA in addition to swarm intelligence algorithms contain connected effectively to an assortment of NP-hard issues. Additionally, with regards to clustered routing within WSN, a few EA methods are present in the literature. GCA (genetic clustering algorithm) is an EA for the dynamic development of clusters in WSNs [39]. The goal of GCA is to expand the lifespan of the network by means of comprising least energy scattering. Within GCA, every chromosome is spoken to as a string of length N, wherever every gene relates to a specific node. The estimation of every gene is able to be $+1$ (showing the node be a CH), 0 (demonstrating the node be a non-CH), or -1 (showing which the node former departed). Jin et al. [40] have proposed another clustering strategy depending on GA endeavor to discover suitable CHs to limit the clustering distances. Within this method, binary encoding is utilized for the chromosome portrayal, in that, every gene relates to one node: 1 implies which comparing node is chosen as a CH, and something else, 0 implies which it is a non-CH node.

To achieve energy efficiency in WSN [41, 42], a new RAP protocol is introduced to enhance the network lifetime using the hybridization of ant colony optimization (ACO) as well as particle swarm optimization (PSO) algorithm. To further enhance the energy effectiveness, the projected RAP algorithm uses a reactive data transmission strategy that is incorporated into the hybridization of ACO and PSO algorithm. In the beginning, the clusters are organized based on the residual energy and then the proposed RAP algorithm will be executed to improvise the inter-cluster data aggregation and reduces the data transmission. In summary, the contributions of the paper are listed below.

- The investigation of the state-of-the-art clustering techniques in WSN takes place.
- From the extensive survey, it is concluded that the efficient data aggregation technique using the hybridization of ACO and PSO algorithms leads to better lifetime.
- A reactive data transmission scheme is also employed to broadcast data alone while the sensed value crosses a threshold limit.
- Simulation results have been analyzed to validate the efficiency of the RAP protocol.

The upcoming sections of the study are formulated as below: The network design is known in Sect. 2, as well as the proposed RAP algorithm, is presented in Sect. 3. The consequences are discussed in Sect. 4 as well as the paper is completed in Sect. 5.

2 Network Model

Some of the assumption made in the proposed work is listed below:

- N sensor nodes are dispensed in the area of M × N.
- Nodes and BS are not mobile.
- Node has its unique ID.
- Symmetric links.

2.1 Energy Model

During the transmission and reception of data, the node has to utilize some energy on the basis of two-channel propagation model known as free space (D2 power loss) in case of single-hop communication and multipath fading channel (D4 power loss) in case of multi-hop communication. So, the energy utilization of the nodes for broadcasting and getting a k-bit packet about a distance d can be represented as

$$E_{TX}(k,d) = \begin{cases} k \times E_{elec} + k \times \varepsilon_{fs} \times d^2 \ if \ d \le d_0 \\ k \times E_{elec} + k \times \varepsilon_{mp} \times d^4 \ if \ d > d_0 \end{cases} \tag{1}$$

$$E_{RX}(k) = l \times E_{elec} \tag{2}$$

where E_{elec} is the dissipated energy in transmitter otherwise receiver circuit, d_0 is the threshold distance that it is estimated through $\sqrt{\varepsilon_{fs}/\varepsilon_{mp}}$. Depending on the broadcast distance d, free space (ε_{fs}) otherwise multipath fading (ε_{mp}) be employed within the transmitter amplifier.

2.2 Cluster Head (CH) Formation

Thus, this study employs the level flanked clustering process where CHs are elected based on a thresholds function. It defines which node by means of higher energy has a high possibility of becoming CHs. Every node will generate a value randomly and tries to turn out to be CH. When the arbitrary value is lower compared to the threshold T (i), it would turn out to be CH. And, T (i) can be represented as

$$T(i) = \frac{P_{opt}}{1 - p_{opt}\left(r.mod\left(\frac{1}{P_{opt}}\right)\right)} * \frac{E_i(r)}{E_{avg}(r)} \tag{3}$$

where r indicates the present round in WSN, E is the present energy of ith node, whereas E. denotes the average residual energy which can be computed as

$$E_{avg} = \frac{\sum E_i(r)}{N} \tag{4}$$

N indicates the count of nodes within WSN.

3 Proposed RAP Algorithm

The RAP algorithm is employed to locate the shortest route out from CHs to BS. ACO and PSO algorithm [43, 44] has the capability to identify the optimized path among a collection of nodes and BS as the destination. Next, reactive strategy reduces the count of data transmission by allowing the data transmission alone while the sensed value is greater than the threshold value.

3.1 ACO Based Path Selection

Here, the least cost based spanning tree (shortest path) is constructed among CHs as well as BS. The steps involved in this algorithm are as follows:

1. Initialization of CHs as ants integrated to BS as the target.
2. Using virtual ant based upon the quantity of pheromone on the CH distances.
3. The beginning of ACO can be the process of collecting trail between nearby clusters, where a number of synthetic ants (CHs) be designed from CHs to BS.
4. At the forefront, ants are selecting the subsequent CH in the random manner by gathering the data out of the length matrix in addition to the successful ants updates the pheromone deposition on the boundaries met by those through an amount (CL), wherever M be the sum of travel time of the ant as well as D a constant price which is altered in continuation by means of the new troubles to the perfect value.
5. The subsequent group of ants follows the leftover pheromone deposition feedback through the previously visited successful ants and quickly follows the shortest route.
6. While ants move from one CH_i to CH_j, the possibility in the selection standard (so known as pheromone) for a simple ant be calculated as follows:

$$P_{ij} = \frac{(\tau_{ij})^{\alpha}(\eta_{ij})^{\beta}}{\sum_{j \in N}(\tau_{ij})^{\alpha}(\eta_{ij})^{\beta}} \tag{5}$$

Here, τ_{ij} indicates the quantity of pheromone deposition from the CH_i to CH_j demonstrates the sum of pheromone deposit from CH_i to CH_j. η_{ij} is the trail visibility function which is equal to the reciprocal function of the energy distance

between CH_i and CH_j, α and β are the parameters to alter the pheromone quantity of τ_{ij} and η_{ij}, respectively.

7. When a link is available between the CH_i to CH_j; then

   P_{ij} gets updated
   else
   $P_{ij} = 0$
   End

8. The distance d_{ij} between CH_i and CH_j can be calculated as follows:

$$d_{ij} = \sqrt{(S(i).xd - s(j)xd)^2 - (S(i).yd - s(j)yd)^2} \tag{6}$$

   Here, xd and yd are the XY coordinates of the given CH.
9. P values get restructured by every ant that has arrived at the BS.
10. Pheromone evaporation ρ on the edge flanked by CH_i along with CH_j be computed employing the Eq. (7).

$$\tau_{ij} \leftarrow (1 - \rho)\tau_{ij} \tag{7}$$

11. For the CHs which are not selected through artificial ants; the measure of P will decrease in an exponential way.
12. In each round (t) = {1, 2, 3, 4…n}, when each and every ant reaches the BS, the value of τ_{ij} will be equated as
    $\tau_{ij}(t + n) = \rho \cdot \tau_{ij}(t) + \Delta\tau_{ij}$. Here, $\Delta\tau_{ij}$ indicates the pheromone quantity getting settled.
13. If ant k have crossed a few edges between CHs, it would depart P that is indirectly relational to the whole distance end to end of every edges ant k have conceded out off the initial CH to the BS through the use of Eq. by using the following formula:

$$\tau_{ij} \leftarrow \tau_{ij} + \sum_{k=1}^{m} \Delta\tau_{ij}^{k}, \quad \forall(i, j) \in L \tag{8}$$

    Here, $\Delta\tau_{ij}^{k}$ is the quantity of P ant k deposited over the visited limits. It is estimated via the following expression:

$$\Delta\tau_{ij}^{k} = \begin{cases} \frac{1}{C^K} \\ 0 \end{cases} \tag{9}$$

14. At present, the path by means of the best P value is chosen as well as assigned as an initial solution.
15. Finally, PSO algorithm will be executed to reduce the path cost again.

3.2 PSO Algorithm

The initialization of PSO begins with the output of the ACO algorithm as particles. Every particle holds the saved data for every coordinate that is associated to obtain the optimized solution by subsequent presented best particles. The goal function of each particle is validated and saved. The fitness range of the present optimal particle is known as pBest. While each and every created population are taken, after that the best range is selected from the created population as well as the specific best solution is known as gBest. This work utilizes the shortest path cost as goal function. In general, PSO tries to modify the speed of each particle to its pBest. The speed is computed by arbitrary definitions that are actually arbitrarily formed counts for velocity to pBest. Each examined particle of PSO contains the data that is given as follows:

- A data represents a global solution that is named as gBest.
- The rate for velocity would represent the quantity of data to be altered.
- pBest value.

1. Initially, it is considered that every CHs as particle that has two dimensions like particle position as well as velocity.
2. Then the solutions are initiated on the basis of random distribution. And, the count of the random solution depend on the population size.
3. Now, determining the fitness value takes place by a fitness function that is the lowest path distance. The distance flanked by two nodes can be computed as

$$D = \sqrt{(x_1 - x_2)^2 - (y_1 - y_2)^2} \tag{10}$$

   (x_1, y_1) is the position values of node 1 as well as (x_2, y_2) is the location rates of node 2. Once the distance is determined, then it is needed to compute the gBest that is shortest aggregate distance for each arbitrary result.
4. Production of fresh particles out off the early locate of random solutions. Arrangement of fresh particles from the elderly ones is the production of a fresh particle:

   4.1. Estimating new velocity:
   The present velocity in use particle is assumed to be the value at that the particle's location is modified and the fresh velocity can be computed as

$$new_v = \omega * old_v + \omega_1\left(lBest_p - cBest_p\right) + \omega_2 + w_2\left(gBest_p - cBest_p\right) \tag{11}$$

   where ω indicates the inertia weight. ω1 and ω2 are fundamental PSO tuning variables, v indicates the velocity, and p is the location value.

   4.2. Estimating the new position of the particle is as follows:

$$new_p = old_p + new_v \tag{12}$$

Finally, the fresh particle (new_v and new_p) will be obtained.

5. Now, the fitness value for new_p is computed by the use of distance of the path.
6. The fitness value of old particle, as well as new particle, undergoes comparison as well as the top one will be chosen for the subsequent iteration:

$$
\begin{aligned}
&If\ new_{fv} > old_{fv} \\
&old_{fv} = old_{fv} \\
&else \\
&old\ particle\ is\ forwarded\ to\ next\ iteration \\
&end
\end{aligned}
$$

7. In each iteration, the best solution will be chosen as pBest. The particle with high fitness value in the present iteration is chosen as pBest solution.
8. The pBest solutions every iterations of the particle in that has highest in the midst of all solutions is chosen as gBest solution. In the end, the gBest solution is selected as the present inter-cluster data aggregation route.

3.3 Reactive Data Transmission

The majority of the on hand protocols broadcast information occasionally in a practical method. It increases the count of data transmission as well as the sensed data would be extremely associated. To enhance the energy efficiency, threshold depended on data transmission (reactive) to be projected. The timeline of the reactive data transmission is shown in Fig. 2.

This approach allows the CH to transmit the attributes to its members and the thresholds are listed below:

Hard Threshold **(HT)**: It is a threshold assessment for an attribute that is being sensed. It is the complete rate of the attribute away from that, the node sensing this assessment should control its broadcaster as well as notify to its cluster head.

Soft Threshold **(ST)**: It is a little modification within the rate of the sensed attribute that immunes the node to knob over its transmitter moreover broadcast. The nodes

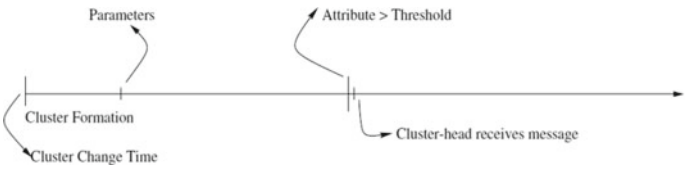

Fig. 2 Time line

sense their environment constantly. The nodes would subsequently broadcast information in the present cluster period, *and* the subsequent circumstances are true:

1. The present rate of the attribute being sensed is higher when compared to the hard threshold.
2. The present rate of the sensed attribute varies from *SV* through a sum equivalent to or superior to the soft threshold. At any time, a node transmits data, *SV* is located equivalent to the in progress value of the sensed attribute.

As a result, the hard threshold minimizes the count of transmissions by allowing the nodes to broadcast alone while the sensed value in the region of significance. The soft threshold additionally minimizes the count of broadcasts through the elimination of every transmission that may contain or else occurred while here is small otherwise no modifications in the sensed attribute on one occasion the rigid threshold.

4 Results and Discussion

The proposed RAP algorithm is implemented in MATLAB and the validation takes place using some metrics. For simulation, 100 sensor nodes are in the area of 100 × 100 m^2. Table 1 depicts the diverse simulation parameters for comparative analysis.

The performance measure throughput indicates the count of packets properly received at the BS. Figure 3 illustrates the comparative results of RAP algorithm with the GSTEB and ACO algorithm. From this figure, it is clearly shown that the RAP algorithm attains maximum throughput than the compared ones. In addition, the inclusion of reactive data transmission acts as a significant task in the improvement of network lifetime. Furthermore, it is verified that the throughput of the RAP algorithm is found to be superior to the existing GSTEB and ACO algorithms.

Table 1 Simulation setup

Parameter	Value
Area (x, y)	100, 100
Base station (x, y)	50, 50 or 50, 150
Nodes (n)	100
Probability (p)	0.1
Initial energy	0.1
Transmitter_energy	$50 * 10^{-9}$
Receiver_energy	$50 * 10^{-9}$
Free space (amplifier)	$10 * 10^{-13}$
Multipath (amplifier)	$0.0013 * 10^{-13}$
Effective data aggregation	$5 * 10^{-9}$
Maximum lifetime	2500
Data packet size	4000

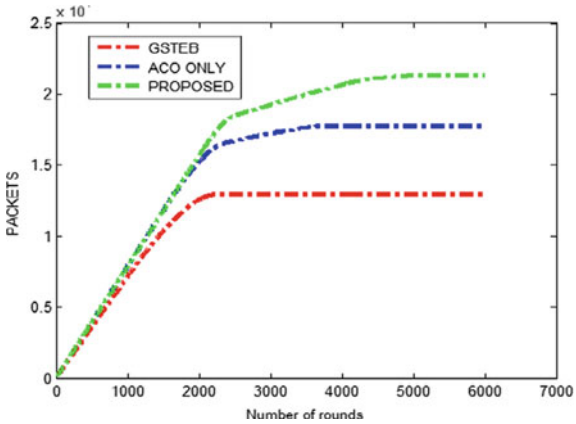

Fig. 3 Throughput

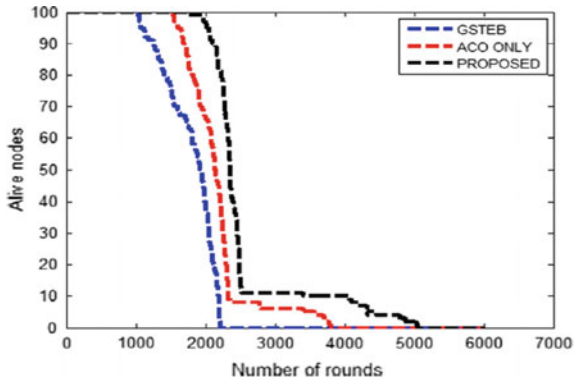

Fig. 4 Analysis of network lifetime

Next, the lifetime of the WSN indicates the time period in between the first as well as last node dies in the WSN. Figure 4 illustrates the comparative analysis of RAP algorithm by means of other methods in terms of lifetime. From the figure, it is clearly depicted that improved lifetime is attained by the RAP algorithm where the network still operates even at 5000 rounds whereas the ACO algorithm makes the network inactive in 3800 rounds itself. It is also apparent that the GSTEB algorithm attains worse performance than the compared methods. On comparing with other algorithms, the RAP algorithm achieved maximum lifetime.

Finally, the residual energy indicates the sum of available energy of all nodes in WSN. Figure 5 provides the comparative results of the proposed RAP algorithm by means of additional algorithms in terms of residual energy. From the figure, it is apparent that the projected RAP algorithm will have maximum residual energy, whereas the GSTEB algorithm achieves minimum residual energy. On the 3000 rounds, the GSTEB algorithm depletes its energy completely whereas the ACO and proposed algorithm have the residual energy of 4 and 7, respectively. From the figures

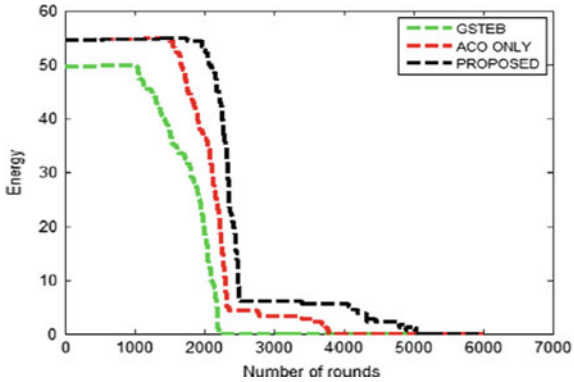

Fig. 5 Analysis of residual energy

and above discussion, it is concluded that the RAP algorithm is found to superior to other algorithms in a significant way.

5 Conclusion

To achieve energy efficiency in WSN, a new RAP protocol is introduced to enhance the network lifetime using the hybridization of ant colony optimization (ACO) as well as particle swarm optimization (PSO) algorithm. To further enhance the energy effectiveness, the proposed RAP algorithm uses a reactive data transmission strategy that is incorporated into the hybridization of ACO and PSO algorithm. In the beginning, the clusters are organized based on the residual energy and then the proposed RAP algorithm will be executed to improvise the inter-cluster data aggregation and reduces the data transmission. The proposed RAP algorithm is implemented in MATLAB and the validation takes place using the subsequent metrics, i.e., stability period, network lifetime, residual energy (average outstanding energy), as well as throughput. The experimental results verified that the RAP algorithm is found superior to other algorithms in a significant way.

References

1. X. Liu, Atypical hierarchical routing protocols for wireless sensor networks: a review. IEEE Sens. J. **15**(10), 5372–5383 (2015)
2. S. Ehsan, B. Hamdaoui, A survey on energy-efficient routing techniques with QoS assurances for wireless multimedia sensor networks. IEEE Commun. Surv. Tutor. **14**(2), 265–278 (2012)
3. O. Younis, M. Krunz, S. Ramasubramanian, Node clustering in wireless sensor networks: recent developments and deployment challenges. IEEE Netw. **20**(3), 20–25 (2006)
4. Y. Mo, B. Wang, W. Liu, L.T. Yang, A sink-oriented layered clustering protocol for wireless sensor networks. Mobile Netw. Appl. **18**(5), 639–650 (2013)

5. M. Elhoseny, X. Yuan, H.K. ElMinir, A.M. Riad, An energy efficient encryption method for secure dynamic WSN, Secur. Commun. Netw. **9**(13), 2024–2031 (2016). https://doi.org/10.1002/sec.1459. (Wiley)
6. M. Elhoseny, X. Yuan, Z. Yu, C. Mao, H. El-Minir, A. Riad, Balancing energy consumption in heterogeneous wireless sensor networks using genetic algorithm. IEEE Commun. Lett. **19**(12), 2194–2197 (2015). https://doi.org/10.1109/lcomm.2014.2381226. (IEEE)
7. Q. Chen, S.S. Kanhere, M. Hassan, Analysis of per-node traffic load in multi-hop wireless sensor networks. IEEE Trans. Wirel. Commun. **8**(2), 958–967 (2009)
8. X. Yuan, M. Elhoseny, H.K. El-Minir, A.M. Riad, A genetic algorithm-based, dynamic clustering method towards improved WSN longevity. J. Netw. Syst. Manag. **25**(1), 21–46 (2017). https://doi.org/10.1007/s10922-016-9379-7. (Springer US)
9. M. Chen, Y. Zhang, Y. Li, M.M. Hassan, A. Alamri, AIWAC: affective interaction through wearable computing and cloud technology. IEEE Wirel. Commun. **22**(1), 20–27 (2015)
10. Y. Zhang, M. Qiu, C.-W. Tsai, M.M. Hassan, A. Alamri, Health CPS: healthcare cyber-physical system assisted by cloud and big data. IEEE Syst. J. **PP**(99), 1–8 (2015)
11. M. Elhoseny, A. Farouk, N. Zhou, M.-M. Wang, S. Abdalla, J. Batle, Dynamic multi-hop clustering in a wireless sensor network: performance improvement. Wirel. Pers. Commun. **95**(4), 3733–3753. https://doi.org/10.1007/s11277-017-4023-8. (Springer US)
12. A. De La Piedra, F. Benitez-Capistros, F. Dominguez, A. Touhafi, Wireless sensor networks for environmental research: a survey on limitations and challenges, in *IEEE EUROCON*, July 2013, pp. 267–274
13. D. Zhang, G. Li, K. Zheng, X. Ming, An energy-balanced routing method based on forward-aware factor for wireless sensor networks. IEEE Trans. Ind. Inform. **10**(1), 766–773 (2014)
14. B. Wang, H.B. Lim, D. Ma, A coverage-aware clustering protocol for wireless sensor networks. Comput. Netw. **56**(5), 1599–1611 (2012)
15. B. Wang, Coverage problems in sensor networks: a survey. ACM Comput. Surv. **43**(4), 32 (2011)
16. M. Elhoseny, A.E. Hassanien, Optimizing cluster head selection in WSN to prolong its existence, in *Dynamic Wireless Sensor Networks*. Studies in Systems, Decision and Control, vol. 165 (Springer, Cham, 2019), pp. 93–111. https://doi.org/10.1007/978-3-319-92807-4_5
17. W. Elsayed, M. Elhoseny, S. Sabbeh, A. Riad, Self-maintenance model for wireless sensor networks. Comput. Electr. Eng. (In Press). https://doi.org/10.1016/j.compeleceng.2017.12.022. Accessed Dec 2017
18. M. Elhoseny, A. Tharwat, A. Farouk, A.E. Hassanien, K-coverage model based on genetic algorithm to extend WSN lifetime. IEEE Sens. Lett. **1**(4), 1–4 (2017). https://doi.org/10.1109/lsens.2017.2724846. (IEEE)
19. B. Singh, D.K. Lobiyal, A novel energy-aware cluster head selection based on particle swarm optimization for wireless sensor networks. Hum.-Centric Comput. Inf. Sci. **2**(1), 1–18 (2012)
20. J. Jin, A. Sridharan, B. Krishnamachari, M. Palaniswami, Handling inelastic traffic in wireless sensor networks. IEEE J. Sel. Areas Commun. **28**(7), 1105–1115 (2010)
21. J. Aweya, Technique for differential timing transfer over packet networks. IEEE Trans. Ind. Inform. **9**(1), 325–336 (2013)
22. J.-D. Tang, M. Cai, Energy-balancing routing algorithm based on LEACH protocol. Comput. Eng. **39**(7), 133–136 (2013)
23. W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks, in *Proceedings of the 34th Annual Hawaii International Conference on System Sciences*, Jan. 2000, pp. 1–10
24. O. Younis, S. Fahmy, HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mob. Comput. **3**(4), 366–379 (2004)
25. Asaduzzaman, H.Y. Kong, Energy efficient cooperative LEACH protocol for wireless sensor networks. J. Commun. Netw. **12**(4), 358–365 (2010)
26. N. Gautam, J.Y. Pyun, Distance aware intelligent clustering protocol for wireless sensor networks. J. Commun. Netw. **12**(2), 122–129 (2010)

27. A. Manjeshwar, Q.-A. Zeng, D.P. Agrawal, An analytical model for information retrieval in wireless sensor networks using enhanced APTEEN protocol. IEEE Trans. Parallel Distrib. Syst. **13**(12), 1290–1302 (2002)
28. S.D. Muruganathan, D.C.F. Ma, R.I. Bhasin, A.O. Fapojuwo, A centralized energy-efficient routing protocol for wireless sensor networks. IEEE Commun. Mag. **43**(3), S8–S13 (2005)
29. K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks. Ad Hoc Netw. **3**(3), 325–349 (2005)
30. X. Gu, J. Yu, D. Yu, G. Wang, Y. Lv, ECDC: An energy and coverage-aware distributed clustering protocol for wireless sensor networks. Comput. Electr. Eng. **40**(2), 384–398 (2014)
31. J. Yu, Y. Qi, G. Wang, X. Gu, A cluster-based routing protocol for wireless sensor networks with nonuniform node distribution. AEU-Int. J. Electron. Commun. **66**(1), 54–61 (2012)
32. J. Yu, Y. Qi, G. Wang, Q. Guo, X. Gu, An energy-aware distributed unequal clustering protocol for wireless sensor networks. Int. J. Distrib. Sens. Netw. **2011** (2011). (Art. no. 202145)
33. A. Chamam, S. Pierre, On the planning of wireless sensor networks: Energy-efficient clustering under the joint routing and coverage constraint. IEEE Trans. Mob. Comput. **8**(8), 1077–1086 (2009)
34. S.K. Singh, M. Singh, D. Singh, A survey of energy-efficient hierarchical cluster-based routing in wireless sensor networks. Int. J. Adv. Netw. Appl. **2**(2), 570–580 (2010)
35. M. Elhoseny, K. Shankar, S.K. Lakshmanaprabu, A. Maseleno, N. Arunkumar, Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Comput. Appl. (2018). https://doi.org/10.1007/s00521-018-3801-x
36. T. Avudaiappan, R. Balasubramanian, S. Sundara Pandiyan, M. Saravanan, S. K. Lakshmanaprabu, K. Shankar, Medical image security using dual encryption with oppositional based optimization algorithm. J. Med. Syst. **42**(11), 1–11 (2018). https://doi.org/10.1007/s10916-018-1053-z
37. S.K. Lakshmanaprabu, K. Shankar, A. Khanna, D. Gupta, J.J. Rodrigues, P.R. Pinheiro, V.H.C. De Albuquerque, Effective features to classify big data using social internet of things. IEEE Access **6**, 24196–24204 (2018)
38. K. Sathesh Kumar, K. Shankar, M. Ilayaraja, M. Rajesh, Sensitive data security in cloud computing aid of different encryption techniques. J. Adv. Res. Dyn. Control. Syst. **9**(18), 2888–2899 (2017)
39. S. Mudundi, H.H. Ali, A new robust genetic algorithm for dynamic cluster formation in wireless sensor networks, in *Proceedings of Wireless and Optical Communications*, Montreal, Quebec, Canada (2007)
40. S. Jin, M. Zhou, A.S. Wu, Sensor network optimization using a genetic algorithm, in *Proceedings of the 7th World Multiconference on Systemics, Cybernetics and Informatics* (2003)
41. M. Elhoseny, A.E. Hassanien, Mobile object tracking in wide environments using WSNs, in *Dynamic Wireless Sensor Networks. Studies*. Systems, Decision and Control, vol. 165. (Springer, Cham, 2009), pp. 3–28. https://doi.org/10.1007/978-3-319-92807-4_1
42. M. Elhoseny, A.E. Hassanien, Expand mobile WSN coverage in harsh environments, in *Dynamic Wireless Sensor Networks*. Studies in Systems, Decision and Control, vol. 165 (Springer, Cham, 2019), pp. 29–52. https://doi.org/10.1007/978-3-319-92807-4_2
43. K. Shankar, P. Eswaran, RGB-based secure share creation in visual cryptography using optimal elliptic curve cryptography technique. J. Circuits Syst. Comput. **25**(11), 1650138 (2016)
44. K. Shankar, P. Eswaran, A secure visual secret share (VSS) creation scheme in visual cryptography using elliptic curve cryptography with optimization technique. Aust. J. Basic Appl. Sci. **9**(36), 150–163 (2015)

Maintaining Consistent Firewalls and Flows (CFF) in Software-Defined Networks

A. Banerjee and D. M. Akbar Hussain

Abstract Software-defined networking (SDN) paradigm brings great flexibility to the network by decoupling control plane from the data plane. However, one of the great security challenges in SDN is to maintain consistency among firewall-rules and actual-flows in the network. The present article proposes one such scheme "consistent firewalls and flows (CFF)" safeguards the network from firewall policy violation and maintains consistency among firewall rules and flow tables. Firewall rule table presented in SDN controller and flow tables present in switches that connect some hosts to the network are treated as critical sections protected by semaphores. We have implemented the CFF framework to demonstrate the efficiency of the proposed scheme and simulation results clearly show benefits of CFF compared to the inbuilt firewall.

Keywords Firewall · Flow table · Security · Semaphore · Software-defined network

1 Introduction

The primary intention behind designing a software-defined network is to implement a centralized control to run various services including packet switching, security mechanisms, network maintenance, etc. The centralized controller, popularly termed as SDN controller is aware of the topology of the whole network. This efficiently decouples control plane from the data plane. OpenFlow protocol [1–5] is mostly used for managing network resources in a cost-effective manner and robust firewalls are required to address security challenges in these types of networks. Firewalls are

A. Banerjee (✉)
Kalyani Government Engineering College, Kalyani, Nadia, West Bengal, India
e-mail: anuradha79bn@gmail.com

D. M. Akbar Hussain
Department of Energy Technology, Section for Power Electronics, Aalborg University, Aalborg, Denmark
e-mail: akh@et.aau.dk

© Springer Nature Singapore Pte Ltd. 2019

M. Elhoseny and A. K. Singh (eds.), *Smart Network Inspired Paradigm and Approaches in IoT Applications*, https://doi.org/10.1007/978-981-13-8614-5_2

widely deployed security mechanisms used in business and institutions. It sits on the border of a network and examines all incoming and outgoing packets to defend against attacks and unauthorized access. A firewall is built based on the assumption that all elements of the protected network are trusted bodies by themselves and internal traffic need not be monitored and filtered. Possible threats to security systems in SDN arise from dynamic updation of network policy, inconsistency between firewall rules themselves, and inconsistency between firewall rules and flow tables at various switches.

(i) Dynamic updation of network policies—In an open flow network, network states are dynamically updated and configurations are frequently changed. These changes have to be reflected in the firewall as well as flow tables. Ideally, flow tables of associated switches have to be modified before centralized firewall rule table because routing decisions are taken at switches through their flow tables.
(ii) Inconsistency between firewall rules themselves—One firewall rule may contradict the other. For example, (A, B, *, allow) and (A, B, *, deny); here A is source-host-id,and B is destination-host-id. Communication between them on all ports is allowed on the first rule and completely denied in the second rule. This is a contradiction.
(iii) Inconsistency between firewall rules and flow table—Let switch sw1 interface host A to the network. Centralized firewall table contains (A, B, *, deny) whereas the flow table of sw1 contains (A, B). Then this is a contradiction between firewall rules and flow table.

The present article proposes CFF which maintains consistency between firewall rules and flow table. This does not require disturbing the SDN controller for accessing the firewall rule table with the arrival of each packet at an ingress switch. Subparts of firewall rules are copied in relevant switches that easily detect prohibited flows. Moreover, firewall rules are stored in such a manner that makes searching for a particular rule efficient. Rules are stored in increasing order of source-host-id and for each source-host-id, multiple destination-host-ids appear in increasing order . Whenever firewall rule table is going to be modified, some parts of the table are locked in write mode while the other entries are free to be accessed for read or write operation. These techniques greatly enhance the performance of the underlying network.

The present article is organized as follows. We overview related work in Sect. 2. Section 3 discusses CFF with an example. Simulation results appear in Sect. 4 while Sect. 6 concludes the paper.

2 Related Work

Some efforts have been made to tackle security issues in SDN. DDoS attack detection [6], vulnerability assessment [7], saturation attack mitigation [8] etc. are important in this context. However, quite differently from them, our work aims to build efficient

firewalls keeping consistency with flow tables of various switches. Floodlight [9] provides us a firewall that stops the undesirable flow of packets at ingress switches depending upon firewall rules "allow" or "deny". However, for each packet flow at the ingress switches, firewall rules present at SDN controller have to be accessed over and over again. This increases the chance of bottleneck at the centralized controller and SDN controller has to be interrupted for every flow, which consumes significant time.

A software extension of FortNOX [10] was proposed for security enforcement in SDN controllers but that did not prove to be very suitable for SDN because FortNOX records rule relations in alias sets, which are unable to track network traffic flows. In [11–14] certain verification tools came up for checking network invariants and policy correctness in OpenFlow but they cannot support automatic and effective violation resolution. Some firewall algorithms and tools have been designed to assist system administrators. Yuan et al. [15] proposed a toolkit to check anomalies or inconsistencies among firewall rules themselves. However, these approaches are not very suitable for software-defined networks.

3 CFF—Explained with an Example

Please consider the network in Fig. 1, consisting of four hosts (A, B, C, D) and seven switches (sw1, sw2, sw3, sw4, sw5, sw6, and sw7). Table 1 specifies firewall rules existing in SDN controller.

In CFF, the controller is equipped with three tables—Firewall-Rules table, Host-Switch table, and Semaphore table. As the name specifies, Firewall-Rules table consists of firewall rules and Host-Switch table consists of host-ids and corresponding switches (switch-id list) that interface a host to the network. For the network shown in Fig. 1, assume that Table 1 shows firewall rules and Table 2 shows Host-Switch table.

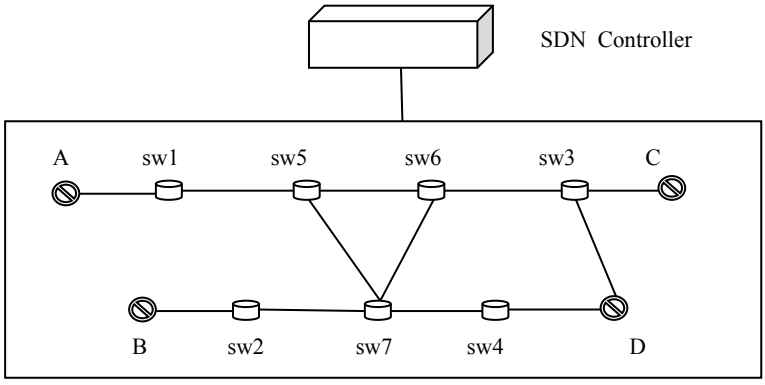

Fig. 1 Example SDN network

Table 1 Firewall Rules table

Source-id	Destination-id	Destination port	Action
A	B	*	Allow
A	C	21, 22	Deny
A	D	21	Allow
B	A	*	Deny
B	C	*	Allow
B	D	23, 25	Deny
C	A	*	Allow
C	B	21	Allow
C	D	*	Deny
D	A	*	Allow
D	B	23	Deny
*	C	*	Deny

Table 2 Host-Switch table

Host-id	Switch-id-list
A	sw1
B	sw2
C	sw3
D	sw3, sw4

Please note that in CFF, firewall rules are arranged in ascending order of source-id and ascending order of destination-id for each source-id.

From the entries of Firewall-Rules table associated with different hosts, two tables named prohibited-flow table and allowed-flow table are constructed corresponding to each switch that interfaces some host to the network. Attributes of prohibited-flow-table are source-id and destination-id whereas the same for allowed-flow-table are source-id, destination-id, and port number. A flow from source H1 to destination H2 will be called prohibited if (H1, H2, *, Deny) is a firewall rule. On the other hand, if firewall rules contain (H1, H2, y, Allow) where y is either * or some port number then (H1, H2) is an allowed flow. Also, if firewall rules contain (H1, H2, y, Deny) where If in the Firewall-Rules table, some port number is mentioned with "Allow" action corresponding to the same source, destination pair, then in allowed-flow table for the same source–destination pair, port number will be positive, whereas for deny action, port number will be negative. For example, in Fig. 1, sw1 interfaces between host A and the network. Therefore, from the firewall rules associated to host A, SDN controller identifies that (A, B), (A, C), and (A, D) are all allowed connections. So, prohibited-flow-table at sw1 is empty and allowed-flow-table is shown in Table 3.

Similarly, prohibited-flow-table and allowed-flow-table for sw2 appear in Tables 4a and 4b, whereas the same tables for sw3 appear in Tables 5a and 5b and for switch sw4, they appear in Tables 6a and 6b.