GUBJSE: ISSN: 2409-0476

SDoT-NFV: A Distributed SDN Based Security System with IoT for Smart City Environments

Md. Jahidul Islam, Anichur Rahman, Sumaiya Kabir, Ayesha Khatun, Ahmed Iqbal Pritom and Mehrab Zaman Chowdhury

Abstract—The Internet of Things (IoT) is a key developing innovation aimed at linking objects via the Internet. While, Software Defined Networking (SDN) is another modern network- ing domain intelligence innovation that increases network effi- ciency and enhances security, reliability, and protection through dynamic software programs. In this paper, we proposed a distributed secure SDoT-NFV architecture for smart cities with Network Function Virtualization (NFV) implementation. We integrated highly protected SDN that delivers better network ef- ficiency, protection, and privacy results. It also secures metadata within each layer as well as payload. In addition, this architecture attempted to implement a more efficient method for constructing a cluster via SDN. Moreover, SDN-IoT with the NFV ideas brings benefits in terms of energy conservation and load balancing to the relevant fields. In addition, several distributed controllers have suggested enhancing accessibility, integrity, anonymity, con- fidentiality, and so on. We also implemented an energy-efficient Cluster Head Selection (CHS) algorithm to make use of our proposed architecture. The network offers greater protection of each network layer as opposed to the traditional network in the proposed architecture. Lastly, we analyze the efficiency of the proposed architecture with different network parameters (throughput, RTT, and Time sequence) for smart cities.

Index Terms—IoT, Smart City, SDN, NFV, Controller, Cluster, OpenFlow, Throughput.

DOI: https://doi.org/10.3329/gubjse.v7i0.54015

This paper was received on 26 April 2020, revised on 22 February 2021 and accepted on 19 April 2021.

M. J. Islam is with the Department of Computer Science and En- gineering, Green University of Bangladesh, Dhaka, Bangladesh. E-mail: jahid@cse.green.edu.bd.

A. Rahman is with the Department of Computer Science and Engineering, National Institute of Textile Engineering and Research, Dhaka, Bangladesh. E-mail: anis.mbstu.cse@gmail.com.

S. Kabir is with the Department of Computer Science and Engineering, Green University of Bangladesh, Dhaka, Bangladesh. E-mail: sumaiya@cse.green.edu.bd.

A. Khatun is with the Department of Computer Science and Engineering, Green University of Bangladesh, Dhaka, Bangladesh. E-mail: ayesha@cse.green.edu.bd.

A. I. Pritom is with the Department of Computer Science and Engineering, Green University of Bangladesh, Dhaka, Bangladesh. E-mail: iqbal@cse.green.edu.bd

M. Z. Chowdhury is with the Department of Computer Science and Engineering, Green University of Bangladesh, Dhaka, Bangladesh. E-mail: mehrab@cse.green.edu.bd

I. Introduction

IN the modern age, we are all connected with devices (billions of IoT [1] devices), we can communicate with each other at any time from anywhere. So the cyber-attacks also increasing because all objects are connected with each other. Vulnerable devices are mostly attacked by intruders. Various technologies are invented in recent years trying to reduce these attacks. Moreover, various researchers have proposed various methods to mitigate the challenges. But it has a lot of problems like security, storage, reliability, flexibility, and Quality of Services (QoS). However, we have to provide a highly secure environment for billion of devices. In recent years IoT is linked with various application areas such as smart grids, VANETs, Smart cities, smart business, and so on. In recent research, it is proved that human beings are connected with thousands of devices (1 man linked with six devices on average).

International Data Corporation (IDC) estimates that by 2022 the IoT market will hit $1.2 trillion. Given the fast advancement of IoT devices which are confronting a few modern security challenges, it is turning into however an- other cybercrime field. Since there are related billions of IoT devices and nearby device-to-devices data is traded over diverse circulated framework and cloud setting. Thus, IoT is an alluring objective for interlopers. Delicate information transmission from such a complex physical framework may turn out to be once in a while powerless on the grounds that information travel through multiple networks, client devices, and distinctive correspondence courses [2].

As an continuous assess, in case 68% of the whole populace begins living in urban zones by 2050, the significance of the smart city concept will increment at that point [3]. The smart cities are becoming increasingly activated and reliant on IoT. In spite of the fact that different shapes of conventional security components are set on the edges of the web, including Firewall, Intrusion Detection, and Prevention Systems (IDS / IPS). But, these structures are no longer enough to protect the internet of the future generation such as IoT [4].

Therefore, SDN [5] is presented as a optimistic innovation along these lines as of late. An convenient approach to IoT-

related privacy concerns is the SDN. The principle normal for this innovation, which provides the addition security with flexibility. It has two planes (Data Plane and Control Plane). It also provides security with multiple controllers (security, application). Moreover, it has secure gateway that enhance the privacy and security. Also, it has several communication protocols. OpenFlow [6] is one of the most common communication synchronisation protocols.

On the basis of the discussion above, we also proposed a stable distributed smart city SDN-IoT network architecture with NFV resolving limitations in traditional network environments. This model enhances the security and privacy of the system where SDN, NFV provides additional security with reliability and flexibility. It also mitigates the cyberattacks from outside of the networks. Also, enhances the network lifetime.

The paper's fundamental contribution is summed up as follows:

- Authors propose "SDoT-NFV" architecture for enhancing security and privacy with NFV implementation for the smart city.
- An energy-aware CHS algorithm is presented that selects the Cluster Heads (CHs) among the IoT devices.
- Moreover, we have addressed an SDN environment which can be capable of enhancing security, scalability as well as privacy of the network.

Organization: In section II, we have presented and examined the recent relevant works. Then, the authors have described the background study in section III. After that, in section IV, the authors suggested a stable SDoT-NFV model for smart cities with an energy-aware CHS algorithm. Moreover, the result analysis is shown in section V. Finally, the authors have concluded the paper with directions in section VI.

II. Related Works

Recently, a remarkable number of researchers are working on the basis of emerging technology like SDN. IoT, NFV, and so on in different applications efficiently. In this section, we have presented some existing research as follows:

A. SDN in IoT Network

A privacy-preserving system has been proposed by Gheisari et al. [7] using SDN-IoT network. The authors mention some privacy issues and try to solve the problem compared with the existing system using mininet-wifi.

An SDN-IoT based method has been proposed by Wang et al. [8] using the benefits of SDN network. Authors consider flexibility and privacy-preserving issues. Also, shows some experiments to prove their work effectiveness.

An IoT-SDN-based control system has been presented by rego et al. [9] for smart cities. Authors try to reduce the time for urban traffic for emergency resources. Moreover, the authors proposed an algorithm for traffic routes and show experimental results using mininet.

In the period 2012 to 2016, An ongoing work [10], Tayyaba et al. (2017) reviewed different proposed SDN answers for IoT. The research also did a comparative examination of different solutions.

For different purposes, Flauzac et al . (2015) [11] have proposed an architecture based on the SDN. Their exploration has concentrated on building up a design to incorporate a wide range of systems like wired, remote, Ad-Hoc, Sensor systems.

Moreover, a stable IoT system based on the SDN has been defined in [12]. Vandan et al. have suggested an IoT environment based security platform using SDN.

B. SDN-IoT with NFV

An SDN-NFV architecture has been presented [13] for security management in IoT networks. Authors mention some security challenges and try to solve using cyber-security tools and technologies. Also, authors successfully implemented and evaluated the system security. They have been designed also a autonomous system using SDN-NFV that monitors the activities.

Authors [14] have been described the open issues and challenges relating to the SDN-NFV in IoT networks. Also, comparing security issues to the conventional networks and providing some future directions.

Another [15] has been analyzed on 4G network using SDN and NFV technologies. They have focused on the energy savings and try to analyze the current research challenges based on the existing works.

C. IoT-SDN based NFV for Smart City

Rahman et al. (2019) have proposed "DistBlockSDN" architecture for smart cities in [16]. Also, authors have presented a secure architecture using an energy aware cluster Head Selection algorithm and shows the experimental results and compare to the existing works.

Another [17] secure architecture has been presented to secure the smart city using smart technologies like SDN, NFV. In that paper, authors analyzed the challenges and presented a architecture to overcome the security challenges using black network.

In similar research, Mukherjee et al. (2020) have proposed SDN based security in the IoT network form smart cities in [20]. Then, they have addressed the cluster head selection strategy for extracting IoT sensor data properly. Further, the authors have used multiple distributed controllers to provide high privacy, integrity, as well as more security to the distributed IoT network efficiently.

Arasteh et al. (2016) have described several concepts of smart cities, motivations, applications, and features after pro- viding a broad, comprehensive overview of different existing works [22]. They also highlighted some typical challenges like security, privacy, heterogeneity, reliability, etc.

From the above premises, we have noticed that several researchers have correctly identified the security problems and

TABLE I: Recent related works analysis

Works	Application areas	Technologies	Security issues	Quality of Services (QoS)	CHS Algorithm
Vandana et al. [12]	IoT Networks	SDN-IoT	✓	×	×
Zarca et al. [13]	IoT Networks	SDN- NFV	✓	×	×
Rahman et al. [16]	Smart City	SDN- NFV	✓	×	✓
Islam et al. [17]	Smart City	SDN- NFV	✓	✓	×
Sinh et al. [18]	IoT Networks	SDN- NFV	×	✓	×
Almustafa et al. [19]	4G Networks	SDN- NFV	✓	✓	×
Mukherjee et al. [20]	Smart City	SDN- NFV	✓	✓	×
Molina et al. [21]	IoT Ecosystem	SDN- NFV	✓	×	×
Proposed	Smart City	SDN- NFV	✓	✓	✓

try to solve the problem using various emerging technologies. Finally, we have compared our proposed architecture with various recent works which are shown in Table I.

III. Background

In the following segment, We provided some research related background study: SDN, NFV model with SDN-IoT.

A. Software Defined Networking (SDN)

Software Defined Networking is a new paradigm , that has a great impact on network building and research activities. SDN can separate control plane from the data plane. In control plane, data can be controlled and management. Fig. 1 shows the SDN basic architecture. Moreover, it facilitates the [23] network evaluation and configuration. Improving network performance and using the network most efficiently assets are main benefits of SDN. Even the data plan computers are run randomly.

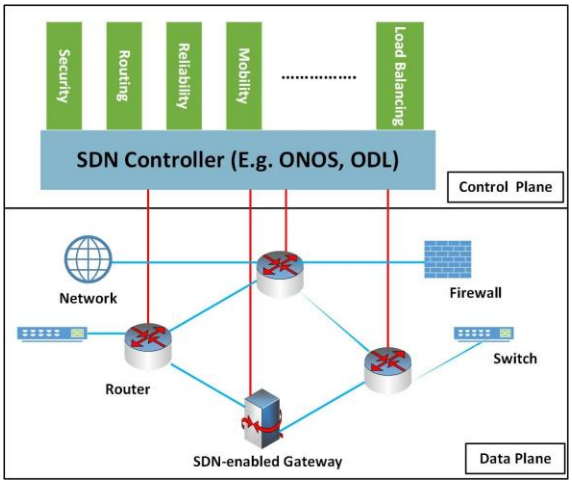

Fig. 1: SDN Architecture

B. SDN Architecture with IoT Network

Adjustment of IoT systems with the SDN design could be a key developing innovation that plays a key part in remote network protection which is shown in Fig. 2. In [24]–[26] , SDN architecture implementations with IoT paradigm. The primary component is the IoT specialist who detects, collects, and analyses the recognition layer data. Based on the essential network consensus, the IoT controller may establish networking rules and regulations and for each regulation, coordinate with the SDN controller. Heterogeneity of devices conquered by the SDN controller as well as observing the approaching and active traffic. SDN regulators alleviate both inside and outer assaults. In this way it can make sure of the biological IoT system proficiently.

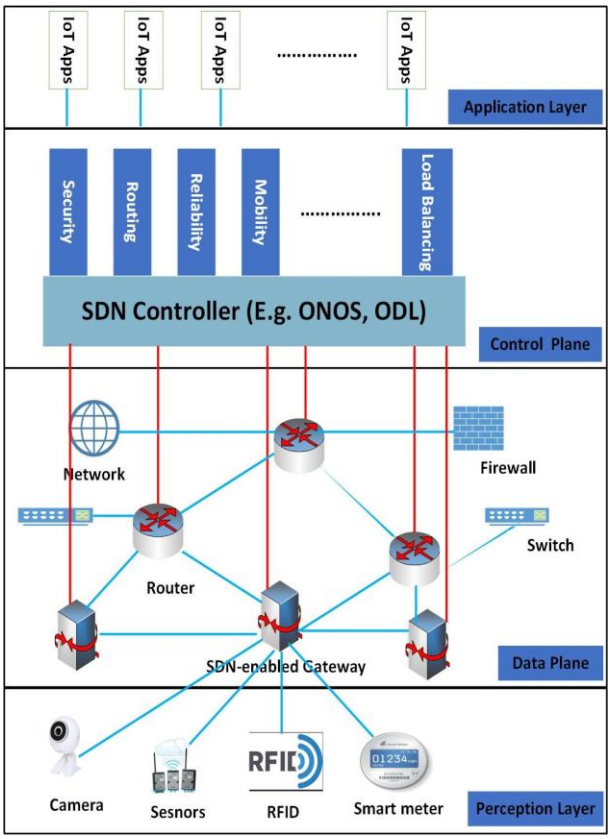

Fig. 2: SDN-IoT Architecture

C. SDN-IoT Architecture with NFV

Network virtualization feature incorporates the concept of utilizing virtual machines that play out the steering, exchanging, and other system works as opposed to utilizing committed equipment as appeared in Fig. 3. Be that as it may, NFV [27] requires to be controlled and organized. In this manner, the SDN accompanies an answer for deal with all the virtual machines and systems by decoupling the control

plane and information plane. IoT framework is conveyed in nature and sensor hubs continue communicating information to regulator applications followed by seeing the earth. This is the explanation, programming characterized IoT biological system usage has been more proficient as far as low force utilization, execution improvement, and decreasing security concerns. The pith of SDN/NFV in the IoT ecosystem system lies in getting better find capacity, productivity, the executives, less complex help affixing, application provisioning, and comprehending interoperability among heterogeneous devices [28]. Authors essentially present software-defined gateway opposed to utilizing customary entryways. However, OpenFlow is a communication protocol which gives the permission of data packets. In this manner, NFV combined with SDN infers less space and force utilization upgrading the presentation of a system in a superior manner.

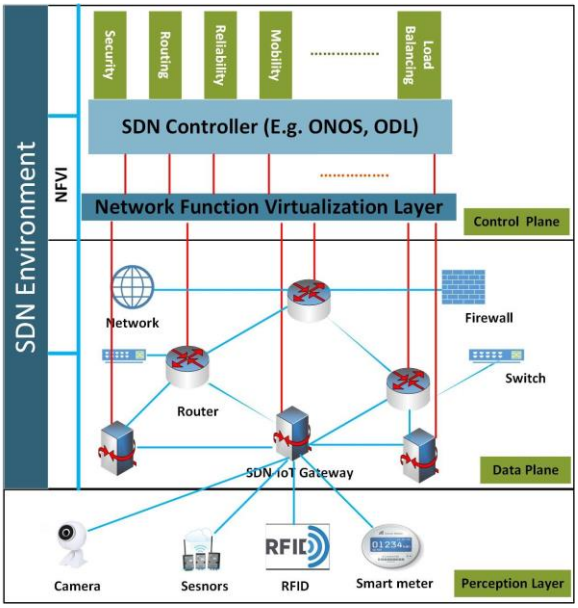

Fig. 3: NFV with SDN [29].

IV. Proposed Model for Smart Cities

In proposed section, we have presented a secure SDN-NFV model that gives the network more security, reliability, and robustness. Moreover, authors presented a energy- aware CHS algorithm. Fig. 4 shows the proposed model.

In the most part, without properly thought out structure, an enormous IoT-based network can not be skilfully cared in. Because of this, we need a cluster concept and think about that there will be a regulator (Cluster design head is called controller). And we have to effectively pick a cluster head from each array. Moreover, clusters select a Gateway Node (GN) that gives the permission for valid node in the cluster domain.

Those domains are defined by:

- An SDN Cluster Head (SDNCH) coordinates a cluster domain.
- SDN Gateway nodes are known as the SDNCH and Sensor Nodes (SN) connective nodes.

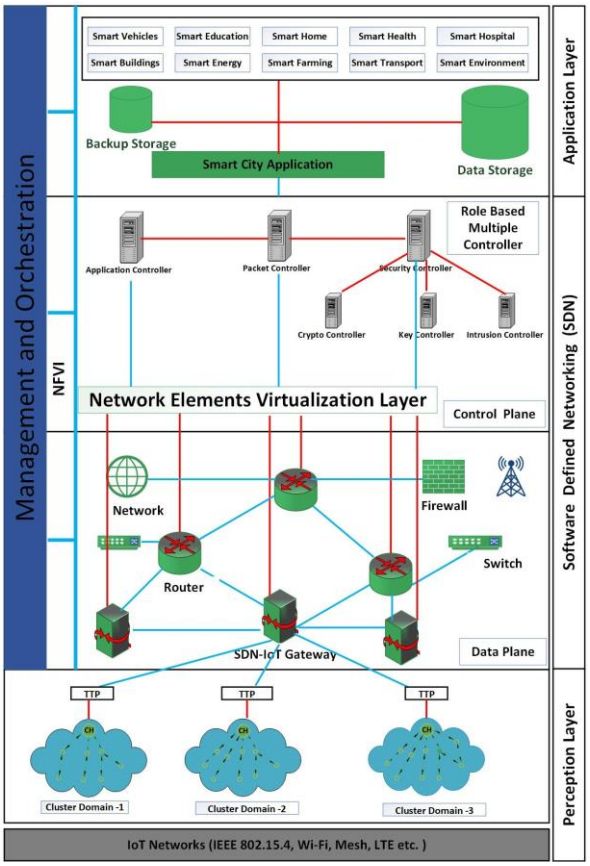

Fig. 4: Proposed "SDoT-NFV" Architecture.

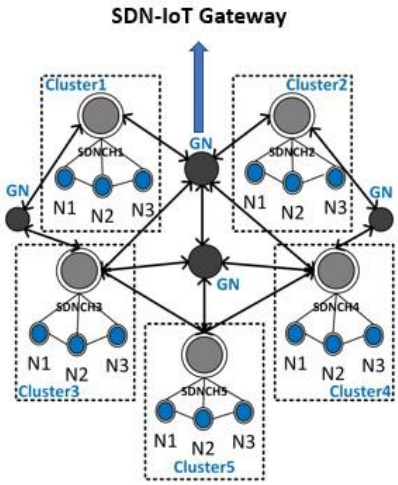

Fig. 5: Clusters Head Selection Process

SDNCH deal with the group area as well as track and productively that secure the cluster domains from the outside attacks. Thus, SDNCH within the cluster domain may be viewed as a security enforcer maintaining the security of the system.

In this section, the authors proposed an energy-efficient cluster head selection algorithm (Algorithm. 1), which shown in Fig. 5. The main goal of the algorithm is to save the energy of each node and send the data to the desired destination

[30]. For increasing the lifetime of the network, Cluster Heads (CHs) are evenly distributed among the network. In the algorithm, we have sorted the IoT nodes with their energy. Then, calculate the distance of IoT devices. After that, we measured the highest energy values among the IoT nodes and lowest distance nodes. Then, primarily considered that the cluster heads among the clusters.

All the sensors node receive the information from the IoT network areas and broadcasting the information by the base station. Before going to sleep, each node transmits data to the CHS. Finally, data sent to the base stations after collecting the data by the CHs through standard SDN gateway. Only can safe and secure CHs reach the destination. Finally, Table II shows the comparison of existing algorithms with our proposed algorithm and Table III also shows the notation of the proposed algorithm.

We have also provided different fundamental building blocks for a smart city with a stable distributed SDN-IoT architecture.

Moreover, to increases the communication connection and network bandwidth as it distributes the data traffic. multiple controller presence eliminates single-point-of-failure incentives. According to the consequence the threats can be mitigated. Some multiple controllers are shown in the following section:

- **Application Controller** The application controller has been configured to track the architecture for malicious use. This controller is decoupled from the packet controller due to its centralized nature, leading to increased risks.
- **Packet Controller** Packet controller used for packet analyzer that creates a restriction zone for packets to enter in the network. It detects the malicious packets and discards from the network.
- **Security Controller**
  - Key Controller: Symmetric and asymmetric keys are maintained by this controller. It is also acted as a key server which is controlled by the TTP.
  - Intrusion Controller: This method is capable of accessibility and safe routing through the maintenance and management of through flow's traffic laws. Mitigation of the infringement is also being undertaken here.
  - Crypto Controller: The fundamental obligations of this module are credibility, anonymity, transparency, authentication, authorization, and identification. This controller requires keys for each operation, ror each operation, a connection with the key controller is needed.

In addition to controlling the cluster domain, the security controller also monitors and ties down each cluster to shield it from the assaults caused both inside and outside. Using the OpenFlow convention, SDN manages all frame interface packets that are based on the parts of the flow table. However, a variety of researchers have been applied to different forms of smart city architecture.

V. Results and Discussions

A. Simulation Setup

For simulation purpose, authors used mininet-wifi. Also, Wireshark used as a packet analyzer where we have used OpenFlow protocol for communication which is shown in Table IV. Authors used 4 SDN Controllers and 2 Gateways with 1 to 50 nodes. We have built a topology in 3000m × 3000m with 800s simulation time. We have evaluated the performance of Average throughput, round trip time, and time sequence(tcptrace).

B. Throughput comparisons

For various number of nodes we have shown average throughput in Fig. 6. For 0-5s the graph is roughly identical. After 6s later the throughput is decreased for less no. of nodes. Since cluster heads can transfer data traffic to the control plane through several gateways, the risk of traffic congestion or inefficiencies within one gateway is greatly reduced also if node numbers increase. Because of this, the topology of 50 nodes relatively offers better throughput distribution opposed with others.

Fig. 7 indicates an similar improvement in the average performance of both networks before they reach 6000bits /s, but upon 5s the performance of extensive MINA decreases unexpectedly, while the performance of 50 topology nodes is comparable. Since the authors have utilized various controllers in the proposed network architecture for appropriate network traffic distribution among the respective controllers, this minimizes time delays and increases network performance. Additionally, network feature virtualization management and orchestration strengthen the network load balancing resulting in better efficiency of the throughput.

C. Round Trip Time Comparisons

For various numbers of nodes, Fig. 8 shows that at the beginning of the time period the RTT is similar. After increasing the time periods the RTT also increases for 10 and 20 nodes but the RTT for 50 nodes are identical or no changes. When it reaches 5-10s that performs worst for different nodes. After that, it performs better for 20-25s. But overall the RTT performs better for 50 nodes in the network.

In addition , the authors compare the 50 node RTT with another [34] OpenFlow based protocol. Illustrate the effect in Fig. 9. It indicates that 50 nodes are needed quite a while before 9s contrast and the OF-based protocol by round trip. But after 10s later, 50-node RTT smoothly decreases compared with the OF-based protocol. There is no question that IoT nodes will connect to SDN-IoT access points via various cluster heads to avoid network congestion for the implementation of the clustering method within the network. As a consequence, network latency is reduced and the round trip time is increased too.

D. Time Sequence (tcptrace) Comparisons

Time Sequence (tcptrace) displays the transmitted TCP metrics like segments and acknowledgments. Fig. 10 indicates

Algorithm 1: Energy Efficiency CHS Algorithm

Input: Υ;
Output: δ;
while (1) **do**
  for $i \leftarrow 1$ *to* $\Upsilon - 1$ **do**
    $min = i$
    for $j \leftarrow i + 1$ *to* Υ **do**
      if $(\Phi[j] < \Phi[min])$ **then**
        $min = j$
      end
      swap(Φ[i], Φ[min]) **end**
    end
    return *Sorted List of Nodes Based on Energy* $(\Phi - \psi)$
    $\zeta \leftarrow G_{dist}(\Phi - \psi)$
    for $i \leftarrow 1$ *to* Υ **do**
      $\delta \leftarrow [\Phi[Max]\zeta]$
    end
    $\Phi_{station} \leftarrow \mu$
    for $i \leftarrow 1$ *to* n **do**
      send request $\leftarrow \delta$
      if $\mu > \Phi_{\delta_1}$ **then**
        send data $\leftarrow \delta_1$
      else if $\mu > \Phi_{\delta_2}$ **then**
        send data $\leftarrow \delta_2$
      else
        send data $\leftarrow \delta_n$
      end
    end
    return δ
  end

TABLE II: Comparison of existing algorithms with algorithm proposed

Works	Node Sorting with Energy Values	Gravity Distance	Latency	Reliability	Energy Savings
Farman et al. [31]	×	×	×	×	✓
behera et al. [32]	×	×	✓	×	×
Jahid et al. [33]	✓	✓	×	✓	✓
Rahman et al. [16]	✓	✓	×	✓	✓
Anich et al. [4]	✓	×	✓	×	✓
Proposed	✓	✓	✓	✓	✓

TABLE III: Algorithm Notations

Parameters	Definition
Υ	Number of Nodes
ψ	Sorted List of Node
Φ	Energy
δ	Cluster Head
G_{dist}	Gravity Distance
ζ	Smallest Distance Separation
$\Phi_{station}$	Energy of Base Station
μ	Assigning Energy

TABLE IV: Environment Setup

Parameters Name	Values
Emulator	Mininet-Wifi 2.2.1
Packet Analyzer	Wireshark
SDN Controllers	4
SDN Gateways	2
Simulation Area	3000m X 3000m
IoT nodes	1-50
Simulation Times	800s
Data Rate	10 Mbps
Packet Size Routing	100-512 bytes
Protocol Measured parameters	OpenFlow Throughput, RTT and Time sequence

that as the number of nodes increases , the number of sequences increases with the time. Consequently the ascent in the grouping number of 50 nodes for geography is more prominent than 10 and 20 nodes.

Moreover, the authors compared the 50 node topology time sequence to the OpenFlow protocol. The result of this is shown in Fig. 11. From 11, it is easy to note that 50 node topology

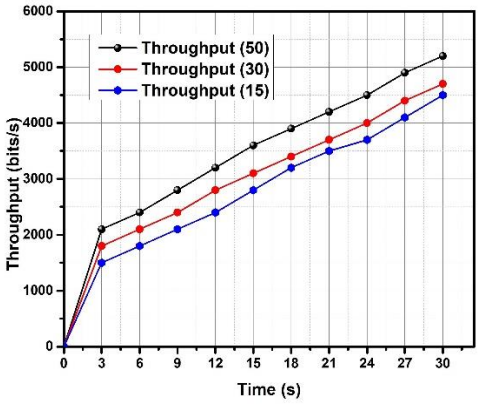

Fig. 6: Throughput Comparison with respect to 15, 30 and 50 Nodes

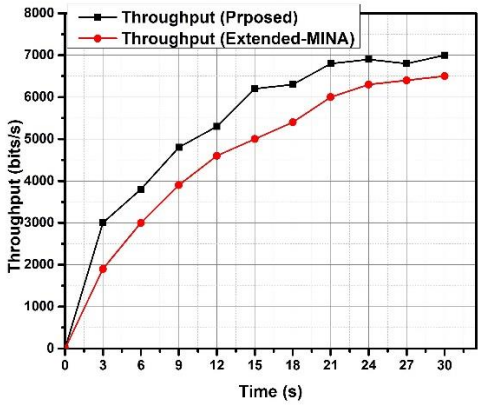

Fig. 7: Average Throughput Comparison for 50 (Proposed) Nodes with respect to Extended MINA

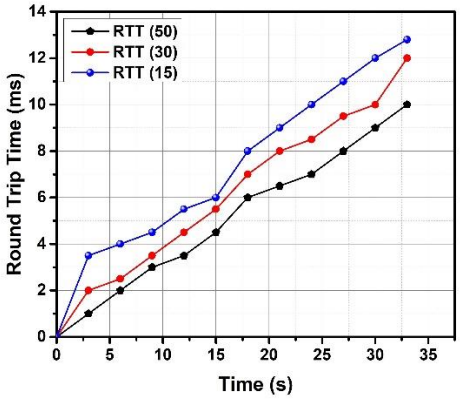

Fig. 8: Round-Trip Delay Comparison with respect to 15, 30 and 50 Nodes

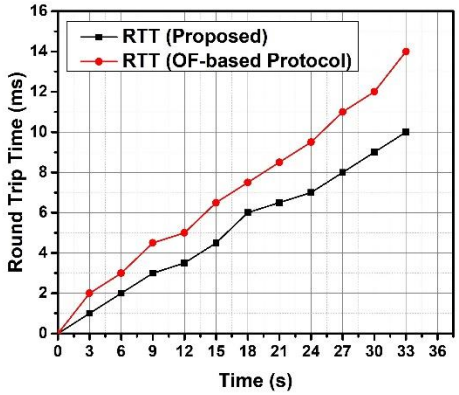

Fig. 9: Round-Trip Delay Comparison for 50 (Proposed) Nodes with respect to OF-based Protocol

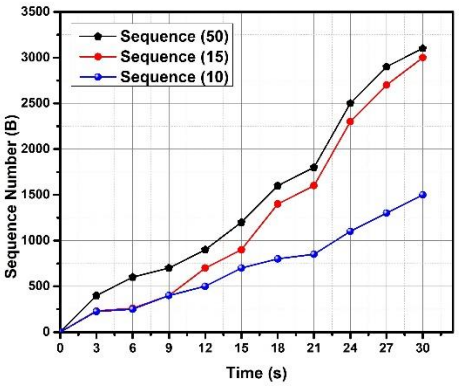

Fig. 10: Time Sequence Comparison with respect to 15, 30, and 50 Nodes

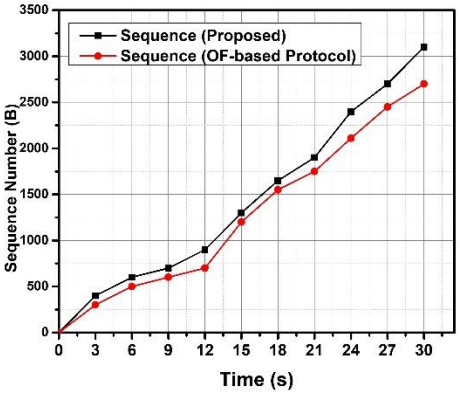

Fig. 11: Time Sequence Comparison for 50 (Proposed) Nodes with respect to OF-based Protocol

provides a smoother time sequence compared to the existing network topology.

VI. CONCLUSION

The technology of the IoT and SDN is still new, and the norms of wellbeing and administration are currently being worked on.

Only a few researchers have addressed some problems in SDN-IoT. Focused on that thought, authors have introduced an effective, safe SDN-IoT model for smart cities using NFV. Multiple distributed controllers have suggested enhancing availability, integrity, safety, confidentiality, authentication, implementation of policies, mitigation, management, and protection overall. In addition, SDN provides an efficient, stable , reliable and versatile IoT solution. Lastly, we introduced the concept of NFV which enhances the network lifetime with power consumption. After all, under the SDN network, overall architecture has regulated that it gets each layer of the system. Furthermore, the proposed architecture can also be used in the implementation of more procedures in the future. But our proposed distributed controller architecture will be excessive congestion and workload problems with routing. But present-day high-speed devices can mitigate this problem.

ACKNOWLEDGEMENT

This work was supported in part by the Center for Research, Innovation, and Transformation (CRIT) of Green University of Bangladesh (GUB).

REFERENCES

[1] H. Rajab and T. Cinkelr, "Iot based smart cities," in 2018 international symposium on networks, computers and communications (ISNCC). IEEE, 2018, pp. 1–4.

[2] Z. A. Al-Sharif, M. I. Al-Saleh, L. M. Alawneh, Y. I. Jararweh, and B. Gupta, "Live forensics of software attacks on cyber–physical systems," Future Generation Computer Systems, vol. 108, pp. 1217–1229, 2020.

[3] K. Kalkan and S. Zeadally, "Securing internet of things (iot) with software defined networking (sdn)," IEEE Communications Magazine, no. 99, pp. 1–7, 2017.

[4] A. Rahman, M. K. Nasir, Z. Rahman, A. Mosavi, S. Shahab, and B. Minaei-Bidgoli, "Distblockbuilding: A distributed blockchain-based sdn-iot network for smart building management," IEEE Access, 2020.

[5] S. Din, M. M. Rathore, A. Ahmad, A. Paul, and M. Khan, "Sdiot: Software defined internet of thing to analyze big data in smart cities," in 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops). IEEE, 2017, pp. 175–182.

[6] A. Prajapati, A. Sakadasariya, and J. Patel, "Software defined network: Future of networking," in 2018 2nd International Conference on Inventive Systems and Control (ICISC). IEEE, 2018, pp. 1351–1354.

[7] M. Gheisari, G. Wang, W. Z. Khan, and C. Fernandez-Campusano, "A context-aware privacy-preserving method for iot-based smart city using software defined networking," Computers & Security, vol. 87, p. 101470,2019.

[8] M. Gheisari, G. Wang, S. Chen, and H. Ghorbani, "Iot-sdnpp: a method for privacy-preserving in smart city with software defined networking," in International Conference on Algorithms and Architectures for Parallel Processing. Springer, 2018, pp. 303–312.

[9] A. Rego, L. Garcia, S. Sendra, and J. Lloret, "Software defined network- based control system for an efficient traffic management for emergency situations in smart cities," Future Generation Computer Systems, vol. 88, pp. 243–253,2018.

[10] S. K. Tayyaba, M. A. Shah, O. A. Khan, and A. W. Ahmed, "Software defined network (sdn) based internet of things (iot): A road ahead," in Proceedings of the International Conference on Future Networks and Distributed Systems. ACM, 2017, p. 10.

[11] O. Flauzac, C. Gonzalez, A. Hachani, and F. Nolot, "Sdn based architecture for iot and improvement of the security," in Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on. IEEE, 2015, pp. 688–693.

[12] C. Vandana, "Security improvement in iot based on software defined networking (sdn)," International Journal of Science, Engineering and Technology Research (IJSETR), vol. 5, no. 1, pp. 2327–4662, 2016.

[13] A. M. Zarca, J. B. Bernabe, R. Trapero, D. Rivera, J. Villalobos, A. Skarmeta, S. Bianchi, A. Zafeiropoulos, and P. Gouvas, "Security management architecture for nfv/sdn-aware iot systems," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8005–8020, 2019.

[14] I. Farris, T. Taleb, Y. Khettab, and J. Song, "A survey on emerging sdn and nfv security mechanisms for iot systems," IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 812–837, 2018.

[15] M. Alenezi, K. Almustafa, and K. A. Meerja, "Cloud based sdn and nfv architectures for iot infrastructure," Egyptian Informatics Journal, vol. 20, no. 1, pp. 1–10, 2019.

[16] A. Rahman, M. J. Islam, F. A. Sunny, and M. K. Nasir, "Distblocksdn: A distributed secure blockchain based sdn-iot architecture with nfv implementation for smart cities," in 2019 2nd International Conference on Innovation in Engineering and Technology (ICIET), 2019, pp. 1–6.

[17] M. J. Islam, M. Mahin, S. Roy, B. C. Debnath, and A. Khatun, "Distblacknet: A distributed secure black sdn-iot architecture with nfv implementation for smart cities," in 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE). IEEE, 2019, pp. 1–6.

[18] D. Sinh, L.-V. Le, B.-S. P. Lin, and L.-P. Tung, "Sdn/nfv—a new approach of deploying network infrastructure for iot," in 2018 27th Wireless and Optical Communication Conference (WOCC). IEEE, 2018, pp. 1–5.

[19] K. Almustafa and M. Alenezi, "Cost analysis of sdn/nfv architecture over 4g infrastructure," Procedia computer science, vol. 113, pp. 130–137, 2017.

[20] B. K. Mukherjee, M. S. I. Pappu, M. J. Islam, and U. K. Acharjee, "An sdn based distributed iot network with nfv implementation for smart cities," 2020.

[21] A. M. Zarca, M. Bagaa, J. B. Bernabe, T. Taleb, and A. F. Skarmeta, "Semantic-aware security orchestration in sdn/nfv-enabled iot systems," Sensors, vol. 20, no. 13, p. 3622, 2020.

[22] H. Arasteh, V. Hosseinnezhad, V. Loia, A. Tommasetti, O. Troisi, M. Shafie-Khah, and P. Siano, "Iot-based smart cities: a survey," in 2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC). IEEE, 2016, pp. 1–6.

[23] S. Bera, S. Misra, and A. V. Vasilakos, "Software-defined networking for internet of things: A survey," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1994–2008, 2017.

[24] A. Rahman, M. J. Islam, M. Saikat Islam Khan, S. Kabir, A. I. Pritom, and M. Razaul Karim, "Block-sdotcloud: Enhancing security of cloud storage through blockchain-based sdn in iot network," in 2020 2nd International Conference on Sustainable Technologies for Industry 4.0 (STI), 2020, pp. 1–6.

[25] A. Rahman, M. J. Islam, Z. Rahman, M. M. Reza, A. Anwar, M. A. Parvez Mahmud, M. K. Nasir, and R. M. Noor, "Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium," IEEE Access, pp. 1–1, 2020.

[26] A. Rahman, U. Sara, D. Kundu, S. Islam, M. J. Islam, M. Hasan, Z. Rahman, and M. K. Nasir, "Distb-sdoindustry: Enhancing security in industry 4.0 services based on distributed blockchain through software defined networking-iot enabled architecture," International Journal of Advanced Computer Science and Applications, vol. 11, no. 9, 2020. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2020.0110980

[27] F. Callegati, W. Cerroni, C. Contoli, R. Cardone, M. Nocentini, and A. Manzalini, "Sdn for dynamic nfv deployment," IEEE Communications Magazine, vol. 54, no. 10, pp. 89–95, 2016.

[28] S. Schaller and D. Hood, "Software defined networking architecture standardization," Computer Standards & Interfaces, vol. 54, pp. 197–202, 2017.

[29] M. Ojo, D. Adami, and S. Giordano, "A sdn-iot architecture with nfv implementation," in Globecom Workshops (GC Wkshps), 2016 IEEE. IEEE, 2016, pp. 1–6.

[30] A. Rahman, M. J. Islam, A. Montieri, M. K. Nasir, M. M. Reza, S. S. Band, A. Pescapè, M. Hasan, M. Sookhak, and A. Mosavi, "Smartblocksdn: An optimized blockchain-sdn framework for resource management in iot," IEEE Access, pp. 1–1, 2021.

[31] A. Ouhab, T. Abreu, H. Slimani, and A. Mellouk, "Energy-efficient clustering and routing algorithm for large-scale sdn-based iot monitoring," in ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020, pp. 1–6.

[32] R. Duo, C. Wu, Y. Tsutomu, and Y. Ji, "Context-aware clustering for sdn enabled network," in 2020 IEEE 28th International Conference on Network Protocols (ICNP). IEEE, 2020, pp. 1–6.

[33] A. Rahman, M. J. Islam, Z. Rahman, M. M. Reza, A. Anwar, M. P. Mahmud, M. K. Nasir, and R. M. Noor, "Distb-condo: Distributed blockchain-based iot-sdn model for smart condominium," IEEE Access, vol. 8, pp. 209 594–209 609, 2020.

[34] Y. Wang and J. Bi, "A solution for ip mobility support in software defined networks," in 2014 23rd International Conference on Computer Communication and Networks (ICCCN). IEEE, 2014, pp. 1–8.

Md. Jahidul Islam received the B.Sc. and M.Sc. degrees in Computer Science and Engineering from Jagannath University (Jnu), Dhaka, in 2015 and 2017 respectively. Currently, he is working as a Lecturer and Program Coordinator (Day) at Computer Science and Engineering (CSE), Green University of Bangladesh (GUB), Dhaka, Bangladesh since May 2017 to present. He is a member of Systems & Security research cell, CSE, GUB. His research interests include Internet of Things (IoT), Blockchain, Network Function Virtualization (NFV), Software Defined Networking (SDN), Digital Forensic Investigation (DFI), HCI, and Wireless Mesh Networking (WMN).

Anichur Rahman was born in Rajbari, Bangladesh, in 1993. He received the B.Sc. degree in Computer Science and Engineering from Mawlana Bhashani Science and Technology University (MBSTU), Tangail, in 2017. Currently, he is working as a Lecturer at Computer Science and Engineering (CSE), National Institute of Textile Engineering and Research (NITER), Savar, Dhaka, Bangladesh since January 2020 to present. His research interests include Internet of Things (IoT), Software Defined Networking (SDN), Image Processing ,Bangla Language Processing, Vehicular Ad-Hoc Networking (VANET), Wireless Mesh Networking (WMN) and Data Mining.

Ms. Sumaiya Kabir was born in Barisal, Bangladesh, in 1989. She received the B.Sc. in Computer Science and Engineering from Patuakhali Science and Technology (PSTU) in 2012 and M.Sc. in CSE from (EWU) in 2017. At present she is working as an Assistant Professor & program coordinator (Day) of department of Computer Science and Engineering in Green University of Bangladesh (GUB) from 2013 to present. She is a member of Systems & Security research cell in CSE, GUB. Her research interest includes semantic web, web 3.0 architecture, ontology designing and semantic knowledge engineering.

Ayesha Khatun was born in Dhaka, Bangladesh in 1994. She received the B. Sc. Degree in Computer Science & Engineering, Chittagong University of Engineering & Technology (CUET). At present she is working as a Lecturer and Program Coor- dinator (Day), Dept. of CSE, Green University of Bangladesh. She achieved scholarship for Higher Study, Wide space Bangladesh Limited, Merit scholarship every year, Department of CSE, CUET. She was also the 2nd Runners up in ICT National Android Application Development Training 2015, Ministry of Information and Communication Technology Division. Her research interests include application of Natural Language Processing, Bangla Language Processing, Data Mining, Artificial Intelligence, and Internet of Things.

Ahmed Iqbal Pritom was born in Dhaka, Bangladesh in 1994. He has been working as a full time faculty member in the department of Computer Science and Engineering at Green University of Bangladesh. His research interest includes Human Computer Interaction, Internet of Things and Data Mining. He has completed his graduation from Islamic University of Technology (IUT), Bangladesh.

Mehrab Zaman Chowdhury is currently working as a Lecturer in the Department of Computer Science and Engineering at Green University of Bangladesh. His research interest encompasses Interaction Design, Assistive Technologies, Human – Machine Interactions. He has completed his graduation from Islamic University of Technology (IUT), Bangladesh.