ANN BASED AUTHENTICATED DATA TRANSFER IN NETWORKS EXPLOITING FUZZY KEY MANAGEMENT

A.Kousalya

Associate Professor, Department of Information Technology,Sri Krishna College of Engineering and Technology,Coimbatore, Tamil Nadu, India. E-mail: kousirakshi@gmail.com

Abstract- Networks for the transfer of data have attracted a lot of attention because of their possible effect on scientific research and various appealing applications. Besides these advantages, security is regarded as a crucial factor during the transmission of data from source to destination. Existing methods for security suffers from issues like key dimension, threat against sensitive details and malicious nodes. Therefore in this paper, an efficient data transfer mechanism exploiting smart grid is designed with the utilization of Fuzzy and ANN. The fuzzy based key generation performs encryption and decryption of the data ensuring authenticated transfer between the nodes. The deep learning ANN approach is utilized which determines the number of hops required to reach the destination thereby providing efficient routing. The obtained results revealed that the proposed methodology for efficient data transfer provided secured data transmission with authenticated routing.
Keywords: Smart grid, Fuzzy, ANN, encryption, decryption.

1 INTRODUCTION

The continuous development of new services, as well as the increase in the amount of knowledge circulating on the Internet, has resulted in the emergence of innovative ideas, theories, and frameworks. Due to the advent of the internet, an overwhelming amount of wired as well as wireless devices have been linked to it, resulting in a faster and broader network flow. Users access the majority of multimedia content in the IP address framework. Even though a network dependent on IP address create communication between two communication hosts, it is not always effective in terms of content delivery. Traditional network infrastructure, on the other hand, which requires policies of improved level network as well as configuration of protocols, is ineffective and has considerable restrictions in terms of scalability, traffic volume, and versatility [1, 2]. Hence various issues, like fragmentation, scattered implementation situations, various requirements, and complexities in the growth of industries as well as applications occur [3, 4].

However, the networks isn't just about sensing and exchanging data. Typically, networks make random decisions depending on sensed data and have increased the efficiency of our living by providing improvement to various fields including smart grids [5-8]. A smart grid (SG) is a viable choice for a traditional power grid's productive energy supply while still increasing its stability and protection. In reality, a legacy power grid's inadequacy communication as well as completely automated control makes it more likely to experience a long and widespread breakdown, which could be triggered by a single faulty component [9]. The Successfully designing as well as implementing efficient, safe, energy-awared as well as infrastructure for cost-effecient communication is critical to realise the potential benefits of smart grid [10]. Smart grids face various threats which are categorized into edge [11, 12], communication [13] as well as power plant [14] layers. The difficulty of launching attacks is linked to threat positioning. Since carrying out attacks at the edge as well as communication layers is much simpler than at a well-protected cloud server, the centralised datacenter is not a common attack target. Sensors are often installed at the network edge and hence an edge layer relates specifically to weaknesses in data collection. Attackers can easily access those sensors and use physical violence against them. Next, attackers deceive controlling nodes or datacenters by interfering with messages or immobilising channels for communication while handling the communication layer threats. In addition, the complexity of attack is high when considering the power plants [15]. Hence there is a need for a robust transmission network equipped with smart grid providing efficient transmission.

Generally, networks utilize various improved services of communication and hence the traffic associated with these services accounts for a significant portion of total network traffic and is growing rapidly. Furthermore, communication networks provide a wide range of facilities as well as carry enormous amounts of data, the network downtime results in a massive data loss, generally critical user data. As a result, it's critical to have certain resiliency mechanisms in the network [16]. Most current work only considers data-forwarding problems like sharing of connection by various content artefacts as well as heavy traffic resulting in congestion when designing caching strategies. If an information object's transmission path from its server to its destination node experiences significant network

congestion, it's critical to cache the content at nodes aside the destination node [17]. In general, real-time routing mechanisms place high demands on various Quality of Services (QoS) metrics such as low latency, maximum throughput, and highly reliable. As a result, these characteristics, as well as other research design aspects like security, accessibility, and coverage, have gotten a lot of attention and are likely to be taken into account [18]. Due to the proprietary hardware function, high operating costs as well as difficulty in changing the present framework, complicated as well as difficult-coded network rles and functions, sluggish and complex network as well as service implementation due to close coupled nature of data planes as well as control in devices and equipment occur [19]. Several methods provide successful delivery rate but utilizes source node as well as two relay nodes for the transmission of data. This requires increased consumption of transmission energy [20]. Hence efficient routing is needed to accelerate and simplify network innovation and deployment.

In addition efficient data transfer is attained by security mechanisms including key-less security and key-based security [21]. The former is achieved by injecting noise artificially [22] as well as with the exploitation of structured interference [23]. The latter utilizes the generation of key for transmission routes considering the attributes like robustness, envelop as well as nature of the data to be transmitted [24]. Therefore, there is a demand for efficient security mechanism based on the generation of key.

Henceforth, an efficient mechanism for data transfer is deigned with the contributions given as,

- Utilization of smart grid for improved reliability and accuracy.
- Adoption of ANN with improved computational costs.
- Fuzzy based key management for encryption and decryption.

The arrangement of paper is: Section 2 elucidates the relevant works. Proposed framework is detailed in section 3. Results as well as discussion are explained in section 4. Finally, work summary is given in section 5.

2 RELATED WORKS

Tanushree et al [25] presented a design as well as implementation of a networking protocol dependent on a communication platform of real time. The time synchronization of estimated data was enabled with the provision of similar time inference for all the estimation devices in the networks. This resulted in a minimal expensive system offering improved security and remained as an appropriate selection for communication systems.

Nasim et al [26] focused on integrated coding of networks with the multi-path transport layer which is reliable in nature for resolving the issues due to traffic. The coding mechanism was proposed for desensitizing the receiver against reordering of packets, subsequently eliminating the traffic issues. The efficacy of the proposed approach was demonstrated by simulation as well as experiment.

Massimo et al [27] considered optimizing of routes as well as spectrally allocating paths in grid exploited networks. On the occurance of traffic the extra complicacy because of the flexible grid revealed lower influence on the complicatedness of the issue. The complexity of the comparison resulted that the gap of performance within the models increased by introducing extra flexibility as well as dimensions.

Alexandre et al [28] investigated the design issues of robust network which faced motivation by the demand for core networks to fulfill the increasing demand for dynamic capacity. The network was designed for exploring the nature as well as range of traffic. The shortest path was designed for the multi hub routing and the carrier possessed the ability to determine the efficient routing path.

Hui-Ming et al [29] comprehensively analysed the security in networks which comprised of authorized users as well as base stations. A secret policy was proposed which associated every user to provide expressions which are tractable. The probability of connection was increased and the probability of secrecy was decreased when a large value of threshold was set.

Daemin et al [30] proposed an optimization protocol offering secured route that permitted the linked devices to communicate directly in a secured manner with minimal leakage of data. The introduced design provided mutual authentication, exchange of key as well as protection of privacy. The verification of security is performed with the analysis of tools and internet protocols.

3 PROPOSED METHODOLOGY

Networks are rapidly gaining traction as low investment remedies for wide issues of real-world. They are constantly expanding, necessitating the implementation of effecacious mechanisms for security. Since networks exchange sensitive data as well as function in hostile, unmonitored regions, these security issues must be tackled from the start of system designing. Sensor network security, on the other hand, faces different obstacles than conventional network security because of resource as well as computational restrictions. Hence there is a need for the efficient design of authenticated system offering secured data transfer with key management.

3.1 Smart Grid in Networks

Smart grid is described as the incorporation of the power grid from the previous inventions with the advancement of information and communication technologies in the present era. Unlike conventional power grids, the smart grid optimises electricity demand delivery, improves reliability, reduces losses, and enables large-scale renewable energy installations such as solar and wind. Every device in the grid is treated as an entity with its own IP address, which can be used to monitor it over internet, allowing for the creation of a smart, self-sustaining ecosystem. By allowing bidirectional information flow as well as synchronisation across the grid system, networks enable a smarter and more integrated grid. Consumers, suppliers, and utility companies may use networks to reduce human interference in controlling smart metres, home gateways, smart plugs, and other appliances connected, indicating that the grid responds to the environment optimally. Figure 1 denotes the model of a smart grid.

The SG is power grid of intelligence and, in the near future, the largest implementation of the network. The complete power grid chain, from energy power plant generation to final electricity users, along with the power transmission and distribution networks, will be equipped with intelligence as well as two-way communication capabilities to remotely track and manage the power grid. Smart appliances, cameras, smart metres, and actuators can be used to achieve this effect. The SG's goal is to maintain a real-time balance between energy generation and consumption by enabling observation and management of the network chain, which is made possible by the large count of smart objects interacting in a two-way manner. Smart grid networks are built by combining a variety of wireless sensors, smart metres, smart appliances, sensors, and other smart items, and all these communicate with one another over a network. In this case, each object is given a unique address so that it can be easily found in the network. It facilitates the transmission of large amounts of data over the internet. It also creates smooth and efficient communication among actuators, sensors, smart metres present at the premises of customer, as well as utility servers, culminating in saving of energy and grid management cost reduction. Utility companies use networks to boost the production and operation of smart grids because it provides enormous promise of a future powered by smart devices that improve performance, ease congestion, and reduce errors. The adoption of SG allows for a large-scale two-way communication flow between the network components. The vast existence of sensors/actuators as well as other smarter objects across the transmitting and distributing areas, as well as the utilization of smart metres and other objects at the customer side, make communication effective. This allows for the real-time tracking of utilization as well as demand to efficient resources, and assisting customers in monitoring their own usage and changing their habits. Networks enable components on the infrastructure of smart grid to be perceived and operated remotely through a communication network which is scalable, allowing for better communication among real world grid components as well as control systems based on computer, improving reliability and accuracy allowing the grid to fulfill the current and future demands.

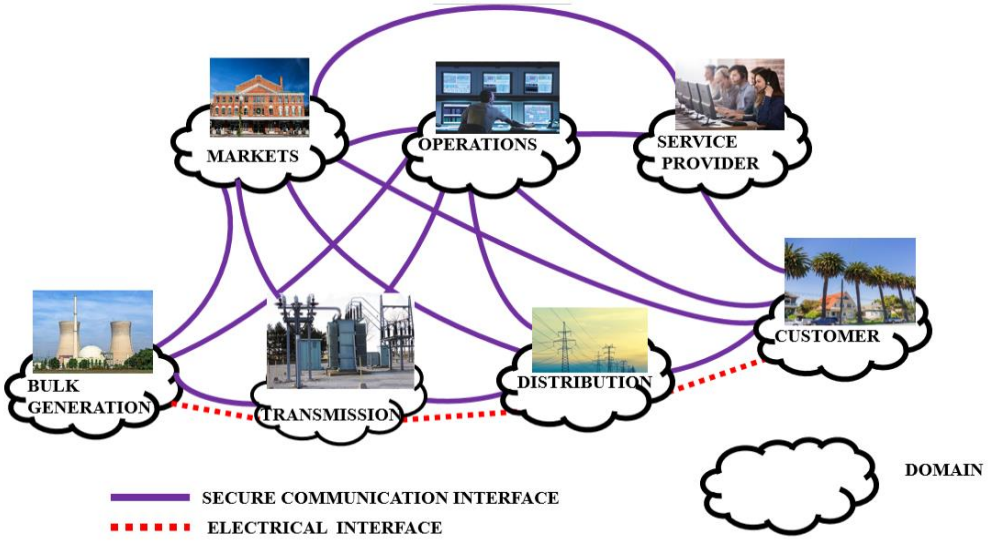

Figure 1 Model of smart grid

3.2 ANN based Routing

ANN is utilized for inferring the routing group of the networks with the synthetic training adopting artificial intelligence. This approach helps in identifying the hop count required for reaching the destination with the observation of topological as well as geometrical attributes of the network. Utilizing ANN provides smarter, quicker as well as advanced way of networking. It exploits statistical methods as well as large data sets for improving the network performance related to a particular task. When lack of mathematical methodology in a network occurs or if the adopted algorithm is very tedious, ANN based approach is utilized. It needs huge database of solutions for issues to initiate the process of learning.

ANN identifies accurately the matching between the input group and the output group where the ANN outputs are considered as variables which are continuous in nature. In this approach, ANN is employed for mapping the number of hops with any routing group depending the message originator, the address of destination and the geometry as well as topology parameters of network. With the utilization of ANN, the computational cost is improved. Figure 2 indicates the ANN utilized for routing.

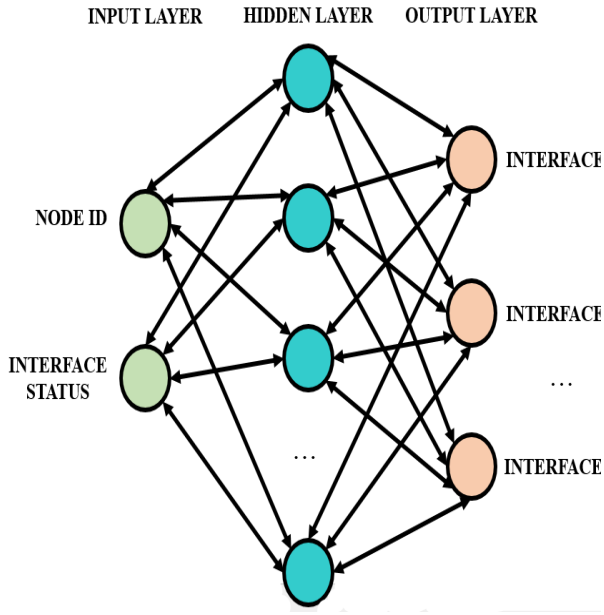

Figure 2 ANN for routing

The mapping within the group of data of numeric inputs and targets is performed by neural networks. To tackle the issue of routing in networks, ANN is utilized. The adopted feed-forward network is of three layered comprising of sigmoid hidden neurons as well as linear resultant neurons for solving multi-dimensional issues. The input data is received by the ANN's input layer in the network. The input data denotes the node ID of the data packet that requires transferring across sensor network. The status of inference denotes the information related to all interface status for a router. Every active interface is utilized for routing data. The communication of data utilizing interfaces which are not active are routed again to interfaces which are active. Certain nodes may face failure of blocking because of power lacking, physical damaging, interferencing of environment. The node failure does not influence the complete network task. When the failure of several nodes occur, the protocols for routing accommodates generation of new connections as well as routes.

The input layer neuron count denotes the information about input for the multilayer perceptron and the hidden layer neuron count is regarded as a optimizing target. The output layer neuron count denotes the router interfaces of the network. The neuron value of the output layer denotes the interface index which is utilized for sending the data packet to destination. The interface will be utilized if the output neuron value is 1, else there occurs no utilization of interface. Interconnection of all layers is performed and there exists no feedback connection within input as well as hidden layers.

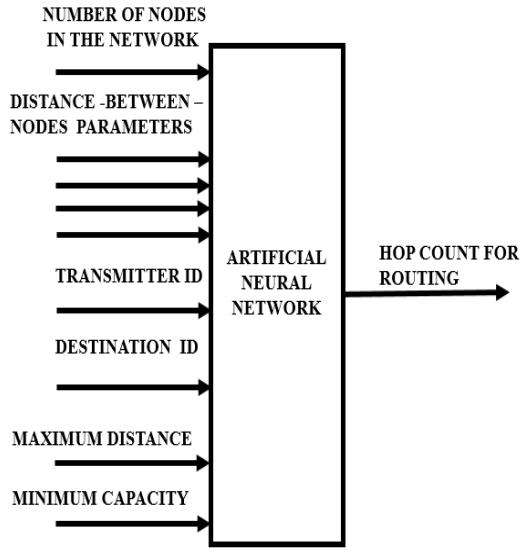

Figure 3 ANN with inputs and output

ANN is utilized for inferring the hop count in the network required for reaching a particular destination. Figure 3 indicates ANN with inputs and output. Generally, most of the ANN inputs are topological in nature and they are given as,

The node count in the network.

- Distance parameters which include mean as well as variance of the powerline cable length utilized for building the infrastructure.
- ID for transmitter in which the the numbering of nodes is performed sequentially starting from left to right.
- ID for destination indicating the node for polling.
- Maximal distance from the central node to a particular node which permits the characterizing of load density.
- Minimal capacity indicating an element which is non-topological in the network.

3.3 Key management based on Fuzzy

Fuzzy theory is regarded as a classical theory extension for elements with varied membership degree. It utilizes the logic of true (1) and false (0) for description. The fuzzy group permits members to possess various membership function degree within the interval (0,1). The selection of key is performed based on fuzzy by the networks with maintaining diverse services. Various data are to be transmitted to the destination and the cipher approach is selected regarding the data size. A threshold data is maintained for deciding the cipher approach and key to be selected. The user performs the selection of key and finds out the key meant for encryption as well as decryption process. The user and the network are responsible for maintaining the value of maximal length of data which is to be utilized.

3.3.1 Fuzzy Encryption

Evaluating in a secret manner while communicating within various networks relates to the functioning effect of users as well as networks. During encryption, the evaluation of the system's security is analysed for which fuzzy is adopted. The corresponding key for encryption is generated and the encrypted file is stored in the memory for the later comparison. The ASCII value of the encrypted data is converted into binary value of 0 and 1.

The process flow is given as,

1) The public key (K, e) of the recipient is received by the sender.
2) Denote the text to its corresponding integer.
3) Change the integer to fuzzy number.
4) Estimate the ciphertext utilizing encryption algorithm

$$C \equiv M^e (mod\ K) \quad (1)$$

5) Apply the exponential operation.
6) Transmit the obtained output.

3.3.2 Fuzzy Decryption

The data encrypted is retrieved from the remote system and the decryption process occurs utilizing symmetric key methodology. The comparison of data is performed with the original data which is further transmitted to the user without any variation.
The process flow is given as,
1) The retrieval of message is performed by applying decryption approach utilizing the private key (K, d)

$$M \equiv C^d (mod\ K) \quad (2)$$

2) Perform the exponential function and the result is converted to fuzzy number.
3) Convert the fuzzy number to representative integer.
4)Convert integer to corresponding text form.

4 RESULTS AND DISCUSSION

Training, validation as well as testing of sets were performed and the sample count for network training relys on router. Every sample is denoted by the rules for routing. One set of rules denote the condition of active states of interface. The other set of rules are utilized at inactive condition of interface. Training was utilized for adjusting the error while the validation set was utilized for measuring the generalization of network. The training phase is not influenced by testing which provides independent network performance measure in and after training. Table 1 indicates the mean square error (MSE) for analyzed ANN. It denotes the average squared variation within outputs and targets and no error results in zero value of MSE.

Table 1 MSE for analysed ANN

No. of hidden neurons	MSE		
	Training	Validation	Testing
10	8.485e-3	2.454e-2	1.525e-1
15	6.953e-2	7.842e-2	9.084e-2
20	7.745e-17	1.082e-16	1.098e-16

Table 2 indicates the regression (R) for analyzed ANN. It denotes the correlation measure within outputs as well as target. A value 1 indicates close relation while 0 indicates random relation.

Table 2 Regression for analysed ANN

No. of hidden neurons	Regression		
	Training	Validation	Testing
10	9.689e-1	9.073e-2	4.224e-1
15	7.456e-1	6.925e-1	6.660e-2
20	9.998e-1	9.998e-1	9.998e-16

The proposed fuzzy based key management is efficacious when compared with existing approaches. The total encryption time extends till the creation of encrypted data and the decryption time continues till the estimation of authenticated data. The fuzzy based approach is compared with cipher based encryption (CBE), Service oriented Multi Model encryption (SMME) and Inner Product Encryption (IPE).

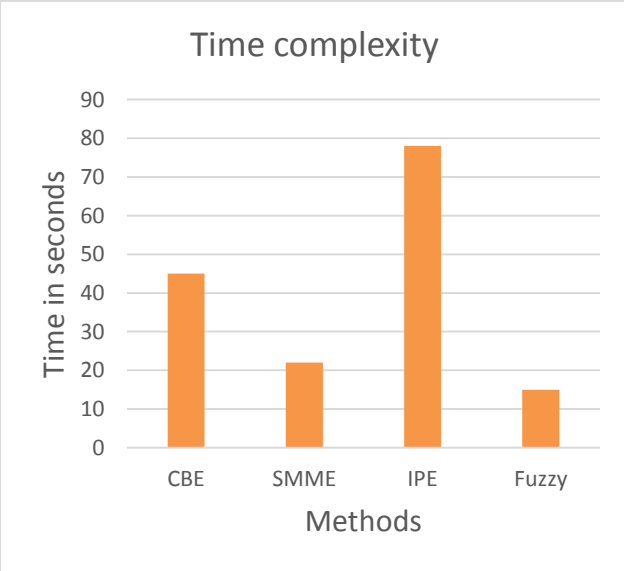

Figure 4 Comparison of time complexity

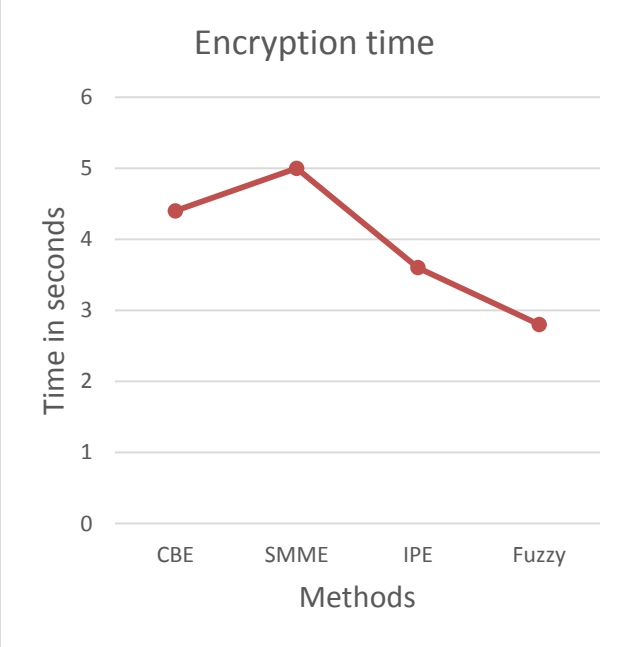

Figure 5 Comparison of encryption time

Figure 4 indicates the comparison of time complexity with existing methods. It clearly indicates that the proposed fuzzy approach generated minimal time complexity.

Figure 5 indicates the comparison of encryption time with existing methods. It clearly indicates that the proposed fuzzy approach consumed minimal time for the encryption of data.

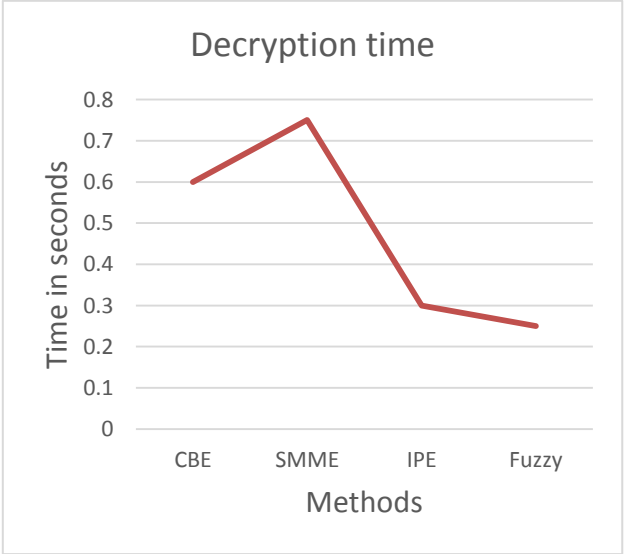

Figure 6 Comparison of decryption time

Figure 6 indicates the comparison of decryption time with existing methods. It clearly indicates that the proposed fuzzy approach consumed minimal time for the decryption of data.

5 CONCLUSION

This paper presented a new approach for efficient data transfer in networks adopting ANN and Fuzzy approaches. ANN was adopted for solving the issues in networks and permits change in routes in case of variations in topology. Fuzzy is adopted for the encryption and decryption of data consuming minimal time. The decrypted output indicated effective security in data transmission ensuring authenticated data transfer. The proposed approach is compared with existing methods and found to be more efficient.

References

[1] Chun-I Fan, I-Te Chen, Chen-Kai Cheng, Jheng-Jia Huang, Wen-Tsuen Chen, "FTP-NDN: File Transfer Protocol Based on Re-Encryption for Named Data Network Supporting Nondesignated Receivers",

IEEE Systems Journal, Vol. 12, no. 1, pp. 473 – 484, 2018.

[2] Yanbing Liu,Yao Kuang,Yunpeng Xiao,Guangxia Xu, "SDN-Based Data Transfer Security for Internet of Things", IEEE Internet of Things Journal, Vol. 5, no. 1, pp. 257 – 268, 2018.

[3] Jin Cao, Pu Yu, Maode Ma, Weifeng Gao, "Fast Authentication and Data Transfer Scheme for Massive NB-IoT Devices in 3GPP 5G Network", IEEE Internet of Things Journal, Vol. 6, no. 2, pp. 1561 – 1575, 2019.

[4] Abhishek Vashist, Andrew Keats, Sai Manoj Pudukotai Dinakarrao, Amlan Ganguly, "Securing a Wireless Network-on-Chip Against Jamming-Based Denial-of-Service and Eavesdropping Attacks", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Vol. 27, no. 12, pp. 2781 – 2791, 2019.

[5] Y. Li, X.Cheng, Y. Cao,D.Wang,and L. Yang,"Smart choice for the smart grid: Narrow band internet of things (NB-IoT) ", IEEE Internet Things Journal., Vol.5 , no.3,pp. 1505-1515, 2018.

[6] L. d.M.B.A.Dib, V. Fernandes, M.de L. Filomeno, and M. V. Ribeiro, "Hybrid pic/wireless communication for smart grids and internet of things applications", IEEE Internet of Things Journal, Vol.5, no.2, pp. 655-667, 2018.

[7] Y. Sun, L. Lampe,and V. W.S.Wong, "Smart meter privacy: Exploiting the potential of household energy storage units", IEEE Internet of Things Journal, Vol.5, no. 1, pp. 69-78, 2018.

[8] H.A.H.Hassan,D.Renga,M.Meo,and L. Nuaymi, "A novel energy model for renewable energy-enabled cellular networks providing ancillary services to the smart grid", IEEE Transactions on Green Communications and Networking, Vol.3, no.2, pp. 381-396, 2019.

[9] Atef Abdrabou, "A Wireless Communication Architecture for Smart Grid Distribution Networks", IEEE Systems Journal, Vol. 10, no. 1, pp. 251 – 261, 2016.

[10] Forkan Uddin, "Energy-Aware Optimal Data Aggregation in Smart Grid Wireless Communication Networks", IEEE Transactions on Green Communications and Networking, Vol. 1, no. 3, pp. 358 – 371, 2017.

[11] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey", IEEE Internet of Things Journal, Vol. 5, no.1, pp.450–465, 2018.

[12] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks", IEEE Transactions on Smart Grid, Vol. 7, no. 1, pp. 530–538, 2016.

[13] K. Gai, M. Qiu, Z. Ming, H. Zhao, and L. Qiu. "Spoofing-jamming attack strategy using optimal power distributions in wireless smart grid networks", IEEE Transactions on Smart Grid, Vol. 8, no. 5, pp. 2431–2439, 2017.

[14] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Dong, "A review of false data injection attacks against modern power systems", IEEE Transactions on Smart Grid, Vol. 8, no.4, pp.1630–1638, 2017.

[15] Keke Gai,Yulu Wu, Liehuang Zhu, Lei Xu, Yan Zhang, "Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks", IEEE Internet of Things Journal, Vol. 6, no. 5, pp. 7992 – 8004, 2019.

[16] Róża Goścień, Krzysztof Walkowiak, Massimo Tornatore, "Survivable multipath routing of anycast and unicast traffic in elastic optical networks", IEEE/OSA Journal of Optical Communications and Networking, Vol. 8, no. 6, pp. 343 – 355, 2016.

[17] Yitu Wang, Wei Wang, Ying Cui, Kang G. Shin, Zhaoyang Zhang, "Distributed Packet Forwarding and Caching Based on Stochastic Network Utility Maximization", IEEE/ACM Transactions on Networking, Vol. 26, no. 3, pp. 1264 – 1277, 2018.

[18] Hasan, Mohammed Zaki, Hussain Al-Rizzo, and Fadi Al-Turjman, "A survey on multipath routing protocols for QoS assurances in real-time wireless multimedia sensor networks", IEEE Communications Surveys & Tutorials, Vol. 19, no. 3, pp. 1424-1456, 2017.

[19] MehranAbolhasan, MahrokhAbdollahi, Wei Ni, Abbas Jamalipour, Negin Shariati, Justin Lipman, "A Routing Framework for Offloading Traffic From Cellular Networks to SDN-Based Multi-Hop Device-to-Device Networks", IEEE Transactions on Network and Service Management, Vol. 15, no. 4, pp. 1516 – 1531, 2018.

[20] Ahmad, Ashfaq, Sheeraz Ahmed, Muhammad Imran, Masoom Alam, Iftikhar Azim Niaz, and Nadeem Javaid, "On energy efficiency in underwater wireless sensor networks with cooperative routing", Annals of Telecommunications, Vol. 72, no. 3-4, pp. 173-188, 2017.

[21] J. Q. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key Generation From Wireless Channels: A Review", IEEE Access, Vol. 4, pp. 614-626, 2016.

[22] F. Shu, L. Xu, J. Wang, W. Zhu, and Z. Xiaobo, "Artificial-noise-aided Secure Multicast Precoding for Directional Modulation Systems", IEEE Transactions on Vehicular Technology, Vol.67, no.7, pp. 6658-6662, 2018

[23] D. A. Karpuk and A. Chorti, "Perfect Secrecy in Physical-Layer Network Coding Systems From Structured Interference", IEEE Transactions on

Information Forensics and Security, Vol. 11, pp. 1875-1887, 2016

[24] Yuanyuan Kong, Bin Lyu, Feng Chen, Zhen Yang, "The Security Network Coding System With Physical Layer Key Generation in Two-Way Relay Networks", IEEE Access, Vol. 6, pp. 40673 – 40681, 2018.

[25] Tanushree Agarwal, Payam Niknejad, M. R. Barzegaran, Luigi Vanfretti, "Multi-Level Time-Sensitive Networking (TSN) Using the Data Distribution Services (DDS) for Synchronized Three-Phase Measurement Data Transfer", IEEE Access, Vol. 7, pp. 131407 – 131417, 2019.

[26] Nasim Arianpoo, Ilknur Aydin, Victor C.M. Leung, "Network Coding as a Performance Booster for Concurrent Multi-Path Transfer of Data in Multi-Hop Wireless Networks", IEEE Transactions on Mobile Computing, Vol. 16, no. 4, pp. 1047 – 1058, 2016.

[27] Massimo Tornatore, Cristina Rottondi, Roza Goscien, Krzysztof Walkowiak, Giuseppe Rizzelli, Annalisa Morea, "On the complexity of routing and spectrum assignment in flexible-grid ring networks [Invited]", IEEE/OSA Journal of Optical Communications and Networking, Vol. 7, no. 2, 2015.

[28] Alexandre Fréchette, F. Bruce Shepherd, Marina K. Thottan, Peter J. Winzer, "Shortest Path Versus Multihub Routing in Networks With Uncertain Demand", IEEE/ACM Transactions on Networking, Vol. 23, no. 6, pp. 1931-1943, 2015.

[29] Hui-Ming Wang, Tong-Xing Zheng, Jinhong Yuan, Don Towsley, Moon Ho Lee, "Physical Layer Security in Heterogeneous Cellular Networks", IEEE Transactions on Communications, Vol. 64, no. 3, pp. 1204 – 1219, 2016.

[30] Daemin Shin, Keon Yun, Jiyoon Kim, Philip Virgil Astillo, Jeong-Nyeo Kim, Ilsun You, "A Security Protocol for Route Optimization in DMM-Based Smart Home IoT Networks", IEEE Access, Vol. 7, pp. 142531 – 142550, 2019.