Inquiry On Data Communication And Access Control In Mobile Virtual Private Network

Author : **R A Vinoth Kumar** , Research Scholar, School of Computer Studies,
Rathnavel Subramaniam College of Arts and Science, Sulur, Coimbatore.

Co-Author : **Dr S Suganya**, Associate Professor, School of Computer Studies,
Rathnavel Subramaniam College of Arts and Science, Sulur, Coimbatore.

ABSTRACT

Mobile computing is a collection of distributed computing systems or service provider servers to participate, link, and synchronize through mobile communication protocols. Virtual private network (VPN) transmits the data over unsecured and shared network infrastructure. VPN is a protected connection between two entities that not directly linked. Mobile virtual private network is a network configuration where mobile devices like notebook computers access intranet while moving from one location to another location. Mobile VPN provides the continuous service to the users and faultlessly switches across the access technologies and multiple networks. Access control is performed to reduce the unauthorized access to physical assets and information system. Many researchers carried out their research for increasing the security level in mobile computing system for virtual private network. However, data confidentiality rate was not increased and execution time was not minimized. In order to address these problems, the existing secured data communication and access control techniques are reviewed.

Keywords: mobile computing, virtual private network, mobile communication, network infrastructure, access control

1. INTRODUCTION

Mobile Computing is a developing topic that comprised the wide spectrum of networked products, systems and sensors with merits of advancements in computing power and network interconnections to provide the new capabilities. The mobile computing is used for the applications like Internet-enabled appliances, home automation components and energy management devices. A mobile VPN is a network configuration where the mobile devices like notebook computers or personal digital assistants (PDAs) access the VPN or intranet moving from one physical location to another. Internet-of-Things (IoT) is a key technology to link massive machines and devices in future communication network. Security is concerned with the protection of message or data while transmitting over networks. Secure communication is defined as the process through which the people share information with different degree of certainty that third parties cannot interrupt.

This paper is organized as follows: Section 2 explains on existing secured data communication and access control techniques in mobile VPN. Section 3 presents the brief discussion about secured data communication and access control techniques in mobile VPN. Section 4 explains the possible comparison between them. Section 5 describes the limitations and related works. Section 6 concludes the paper.

2. LITERATURE REVIEW

An effective-throughput and effective-amount-of-information was employed in [1] to balance the transmission rate and packet error rate for improving the transmission efficiency and reliability. But, the communication overhead was not reduced. A Spectrum aware Energy-Efficient multi-hop multi-channel routing scheme (SpEED-IoT) was designed in [2] for D2D communication in IoT mesh network. A multi-hop routing scheme detected best route, best channels at each hop along route and optimal transmission power. But, designed scheme was not used for different primary environments and IoT networks.

The data scheduling from various IoT devices to access point (AP) were carried out in [3] with heterogeneous data features like data freshness, data length, data uploading period and energy state of IoT device. Though energy consumption was reduced, computational complexity was not minimized. A greedy algorithm was presented in [4] through compact attack graphs to detect the cost-effective solution to preserve the IoT systems. Though computational cost was reduced, execution time was not minimized. Base and temporal exploitability scores of CVSS were not joined to determine the success probabilities through considering the inherent and time-dependent features.

A sample crop test-bed comprised irrigation schedule, neural net decision making and remote data viewing in [5]. But, the natural resource failed to justify the utilization of the automatic systems. The computational cost was not reduced. Function-based Access Control scheme in IoT (IoT-FBAC) was introduced in [6] with Identity-based Encryption (IBE) scheme. But, the dynamic access control scheme failed to describe the secure efficient solution to verify validity of linked devices in IoT.

3. SECURED DATA COMMUNICATION AND ACCESS CONTROL IN MOBILE VIRTUAL PRIVATE NETWORK

Mobile Computing is a virtualization technology that distributes the computing resources through Internet. VPN gained secure access into enterprise private network to minimize the cost and increase the performance. VPN is employed to describe the communication network with combination of strong encryption and tunneling technologies to secure the connection. It allowed the enterprises to transport their private data\network services through public infrastructure networks. Security in data communication is an essential one when message transfer between sender and receiver is required to be kept confidential. Secure data communication is an essential problem in message transmission over the networks. Secure data transmission denotes the data transfer like confidential information over the secure channel. Cryptography is used for attaining confidentiality in message transfer. Cryptography is the process of secret writing to preserve the data or message from intruder.

3.1 Resource Allocation for Wireless-Powered IoT Networks with Short Packet Communication

A wireless-powered IoT network (WPIN) with short packet communication (SPC) was carried out with hybrid access point (HAP) to transmit the power to IoT devices wirelessly. The devices transmitted their short data packets attained through finite bloklegnth codes to HAP by harvested energy. SPC experienced from transmission rate degradation and packet error rate. The resource allocation was carried out depending on Shannon capacity attained by infinite blocklength codes. An effective-throughput and effective-amount-of-information were employed to balance transmission rate and the packet error rate for increasing the transmission efficiency and reliability. The designed information jointly optimized transmission time and packet error rate of every user to increase the total effective-throughput or reduce the transmission time subject to the user individual effective-amount-of-information needs. An efficient algorithm was introduced to identify the high-quality suboptimal solution to address the non-convexity of formulated problem.

A total effective-throughput maximization problem was addressed with transmission time and packet error rate of every user. The optimization issue was non-convex because of two reasons: The optimization problem has integer requirement on packet length for making problem as the mixed integer programming. The objective function was not concave with respect to the packet length and packet error rate of every user. It caused an intractable complexity to attain the optimal solution. An efficient algorithm was introduced depending on the block coordinate descent (BCD) principles and concave-convex procedure (CCCP) to address the issues sub-optimally in an iterative method. Total transmission time minimization problem was addressed with transmission time and packet error rate of every user as variables. A minimum effective amount-of-information constraint was considered for every user to guarantee their quality of service. The optimization problem was non-convex and hard to solve optimally. The convergence and complexity analysis of designed algorithm was carried out in efficient manner.

3.2 SpEED-IoT: Spectrum aware energy efficient routing for device-to-device IoT communication

Spectrum aware Energy-Efficient multi-hop multi-channel routing scheme (SpEED-IoT) was introduced for D2D communication in IoT mesh network. The knowledge of radio environment map (REM) was obtained through dedicated spectrum sensors that collect the spatio-temporal spectrum usage. A multi-hop routing scheme was introduced to identify the best route, available channels at every hop along route and optimal transmission power for every hop. SpEED-IoT developed an evolutionary game theoretic route allocation model to maintain parallel D2D communication. SpEED-IoT guaranteed the licensed incumbent protection, IoT device energy preservation, efficient end-to-end data rate optimization as well as fast convergence assignment among the interfering D2D communication. SpEED-IoT was improved for guaranteeing the connectivity and reachability among IoT devices under different spectrum usage conditions.

SpEED-IoT used Environmental Sensing Capability (ESC) to sense and construct spectrum map for employing spectrum availability information in order to identify the best possible end-to-end routes in terms of intermediate hops and best channel to utilize at every hop. The sensors calculated optimal power for every device channel to preserve the primary incumbents and ongoing secondary IoT communications in vicinity. The transmission power control in SpEED-IoT utilized the selective flooding technique to limit overhead of route request forwarding and to preserve energy resources of IoT devices. SpEED-IoT increased end-to-end network performance parameter, namely achievable data rate. SpEED-IoT introduced evolutionary game theoretic approach to interfere end-to-end D2D routes for secondary IoT end-to-end route assignment. The sensors improved the network performance and fairness when equilibrium exists through analyzing the game.

3.3 Energy harvesting-based data uploading for Internet of Things

The data uploading from tremendous devices is the most demanding tasks for Internet of Things (IoT) because of heterogeneous data features and energy limitations of IoT devices. The data uploading problem were studied from two tiers. In first tier, the data uploading get scheduled from different IoT devices to particular access point (AP) through considering the heterogeneous data features like data freshness, data length and energy state of IoT device. In second tier, selection was carried out among diverse APs for one IoT device. An AP selection algorithm was introduced and proved that AP selection process reach the stable state.

A three-layer network framework was introduced based on scheduling process of data uploading from two tiers. In three-layer framework, IoT devices with short-range wireless transmission capability belong to the bottom layer. The access points (AP) with large range transmission capability belong to middle layer. The backbone networks like cellular base station or cable-based computer network belong to the top layer. Every IoT device accesses to suitable AP for data uploading. Each AP functioned as controller that schedules data uploading of accessing devices and guaranteed the AP spectrum efficiency. AP selection processes get into the stable state. Central slot utilization and distributive AP selection algorithm were introduced for IoT devices to attain joint optimization on data uploading and energy harvesting.

4. COMPARISON OF SECURED DATA COMMUNICATION AND ACCESS CONTROL IN

MOBILE VIRTUAL PRIVATE NETWORK & SUGGESTIONS

In order to compare the secured data communication and access control techniques for disease prediction, number of data is taken to perform the experiment. Various parameters are used for enhancing the performance of secured data communication and access control techniques in mobile virtual private network.

4.1 Execution Time

Execution time is defined as the amount of time taken to perform the secured data communication in mobile virtual private network. It is defined as the difference of ending time and starting time of data communication. It is measured in terms of milliseconds. It is given by,

$$Execution\ Time = Ending\ time - Starting\ time\ of\ data\ communication \quad (1)$$

From (1), execution time is calculated. When the execution time is lesser, the method is said to be more efficient.

Table 1 Tabulation for Execution Time

Number of data (Number)	Execution Time (ms)		
	Throughput and effective-amount-of-information	SpEED-IoT Scheme	Three-layer network framework
10	25	34	40
20	27	36	43
30	29	39	46
40	26	37	44
50	24	35	42
60	25	36	43
70	29	38	46
80	31	40	49
90	33	42	52
100	37	44	55

Table 1 describes the execution time with respect to number of cloud user requests varying from 10 to 100. Execution time comparison takes place on existing throughput and effective-amount-of-information, Spectrum aware Energy-Efficient multi-hop multi-channel routing (SpEED-IoT) scheme and Three-layer network framework. The graphical analysis of execution time is illustrated in figure 1.

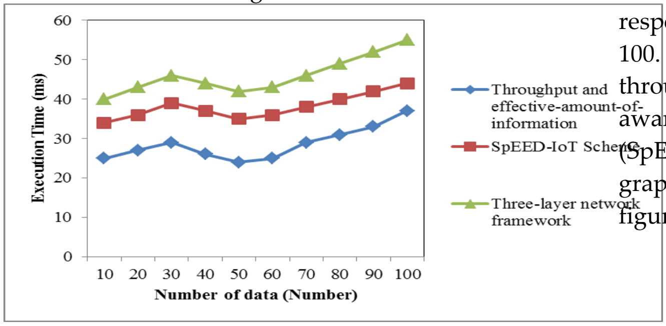

Figure 1 Measurement of Execution Time

As described in figure 1, execution time for different number of data is explained. As described in figure, it is observed that throughput and effective-amount-of-information consumed lesser execution time when compared to the SpEED-IoT Scheme and three-layer network framework. This is because of implementing the block coordinate descent (BCD) principles and concave-convex procedure (CCCP) to address the problems sub-optimally in iterative system. A minimum effective amount-of-information constraint was considered for each user to guarantee the quality of service. Research in throughput and effective-amount-of-information reduces the execution time by 25% than SpEED-IoT Scheme and by 38% than three-layer network framework.

4.2 Energy Consumption

Energy consumption is defined as the amount of energy consumed for secured data communication in mobile virtual private network. It is defined as the product of number of data and energy consumed by one data. It is measured as joules (J). It is given by,

$$Energy\ Consumption = Number\ of\ data * energy\ consumed\ by\ one\ data \quad (2)$$

From (2), energy consumption is calculated. When the energy consumption is lesser the method is said to be more efficient.

Table 2 Tabulation for Energy Consumption

Number of data (Number)	Energy Consumption (J)		
	Throughput and effective-amount-of-information	SpEED-IoT Scheme	Three-layer network framework
10	36	25	45
20	39	28	47
30	41	30	49
40	43	32	51
50	45	35	53
60	47	38	55
70	49	40	58
80	51	43	61
90	53	45	63
100	57	48	66

Table 2 describes the energy consumption with respect to number of cloud user requests varying from 10 to 100. Energy consumption comparison takes place on existing throughput and effective-amount-of-information, Spectrum aware Energy-Efficient multi-hop multi-channel routing (SpEED-IoT) scheme and Three-layer network framework. The graphical analysis of energy consumption is illustrated in figure 2.

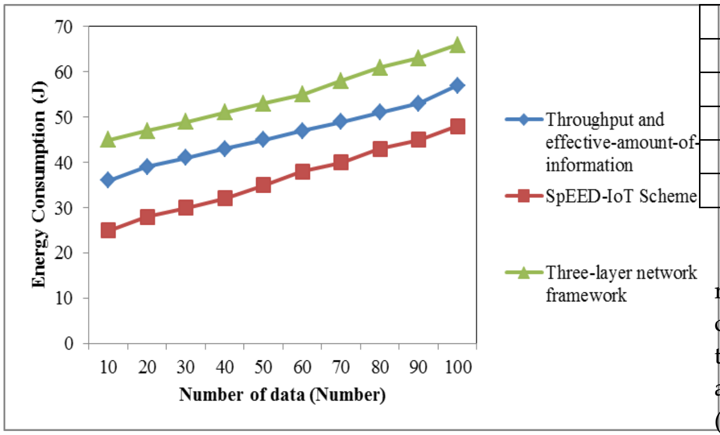

Figure 2 Measurement of Energy Consumption

As described in figure 2, energy consumption for different number of data is illustrated. From the figure, it is observed that SpEED-IoT Scheme consumed lesser energy when compared to the throughput and effective-amount-of-information and three-layer network framework. This is because, SpEED-IoT carried out the data rate optimization of allocated routes and overall IoT network to improve the efficiency in licensed incumbent protection. It enhanced the fairness degree while allocating the routes to multiple interfering devices for reducing the energy consumption. Research in SpEED-IoT Scheme reduces energy consumption by 22% than throughput and effective-amount-of-information and by 34% than three-layer network framework.

4.3 Data confidentiality rate

Data confidentiality rate is the capability to preserve the data for secured communication in mobile virtual private network. It is described as ratio of number of data that are accessed only by authorized user in mobile virtual private network to the total number of data. It is measured in terms of percentage (%). It is formulated as,

$$DCR = \frac{Number\ of\ cloud\ user\ request\ accessed\ by\ authorized\ server}{Number\ of\ data} 100 \qquad (3)$$

From (3), the data confidentiality rate is calculated. When data confidentiality rate is higher, the method is more efficient.

Table 3 Tabulation for Data Confidentiality Rate

Number of data (Number)	Data Confidentiality Rate (%)		
	Throughput and effective-amount-of-information	SpEED-IoT Scheme	Three-layer network framework
10	75	80	89
20	74	79	87
30	72	77	85
40	70	76	82
50	69	74	80
60	66	73	79
70	64	72	77
80	62	71	76
90	59	69	74
100	58	67	72

Table 3 describes the data confidentiality rate with respect to number of data varying from 10 to 100. Data confidentiality rate comparison takes place on existing throughput and effective-amount-of-information, Spectrum aware Energy-Efficient multi-hop multi-channel routing (SpEED-IoT) scheme and Three-layer network framework. The graphical analysis of data confidentiality rate is explained in figure 3.

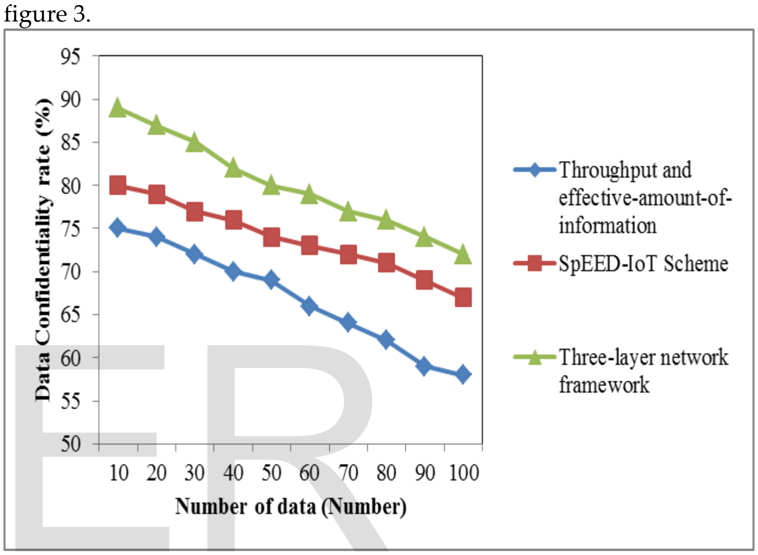

Figure 3 Measurement of Data confidentiality Rate

From figure 3, data confidentiality rate for different number of data is illustrated. It is clear that three-layer network framework has higher confidentiality rate when compared to the throughput and effective-amount-of-information and SpEED-IoT Scheme. This is because of using scheduling algorithm where the emergency function was described for every data uploading need through considering the data freshness, data length, data uploading period and energy level of an IoT device. Every IoT device accessed to AP to present highest predictable data uploading probability. Research in three-layer network framework increases the data confidentiality rate by 20% than throughput and effective-amount-of-information and by 8% than SpEED-IoT Scheme.

5. DISCUSSION AND LIMITATIONS ON SECURED DATA COMMUNICATION AND ACCESS CONTROL

An effective-throughput and effective-amount-of-information were used to balance the transmission rate and packet error rate. It optimized the transmission time and packet error rate of every user to improve the total effective-throughput or to minimize the transmission time with user individual effective-amount-of-information needs. The designed algorithm identified the high-quality suboptimal solutions for solving the non-convexity problem. But, the communication overhead was not minimized. Three-layer network framework was introduced for data upload scheduling from different IoT devices to particular access point (AP) through considering the heterogeneous data features. The designed algorithm improved the successful data uploading rate and time slot utilization. Though the energy consumption was reduced, computational complexity was not minimized.

Spectrum aware Energy-Efficient multi-hop multi-channel routing scheme was introduced for D2D communication in IoT mesh network. The radio environment map (REM) was achieved through spectrum sensors that gathered the spatio-temporal spectrum utilization. SpEED-IoT guaranteed connectivity and reachability among IoT devices under different spectrum usage conditions. But, the designed scheme was not employed for different primary environments and IoT networks in spectrum bands, primary transmission features, spectrum features and heterogeneous secondary IoT device communication capability.

5.1 Related Works

A crowdsourcing method was introduced in [7] for location aware security access (LaSa) control to confine the wireless network access inside physical areas using single commercial Access Point (AP). However, the different techniques were not considered for user moving pattern discovery and aimed complicated indoor cases in LaSa applications. The features of smart devices were employed in [8] to enhance the security of access control technique. The features seamlessly incorporated the dynamic attributes to access control scheme. However, sensor data collection processing determined values for dynamic attributes increased time or communication complexity.

A fine-grained EHR access control scheme was introduced in [9] for increasing the security level under decisional parallel bilinear Diffie–Hellman exponent assumption. But, designed scheme failed to construct fine-grained EHR sharing system for supporting offline key generation, offline encryption and offline decryption at the same time. Time Division Multiple Access (TDMA)-based access scheme was introduced in [10] to allocate resources to heterogeneous nodes. The designed model failed to process the energy consumption function that decrease with compression ratio. In addition, it failed to examine the packet loss on network performance when Shannon limit on channel capacity was not used.

5.2 Future Direction

The future direction of the work can be carried out using cryptographic techniques for secured data communication and access control in mobile virtual private network with higher data confidentiality and lesser time consumption.

6. CONCLUSION

A comparison of different data communication and access control in mobile virtual private network is studied. From survival study, the communication overhead was not minimized. In addition, designed scheme was not used for different primary environments and IoT networks in spectrum bands, primary transmission features, spectrum features and heterogeneous secondary IoT device communication capability. Though the energy consumption was reduced, computational complexity was not minimized. The wide range of experiments on existing techniques computed the comparative results of different cryptographic techniques with its limitations. Finally from the limitation identified, further research work can be carried out for improving the performance of data confidentiality and execution time during the data communication and data access in mobile virtual private network by cryptographic techniques.

REFERENCES

[1] Jie Chen, Lin Zhang, Ying-Chang Liang, Fellow, Xin Kang and Rui Zhang, “Resource Allocation for Wireless-Powered IoT Networks with Short Packet Communication”, IEEE Transactions on Wireless Communications, Volume 18, Issue 2, February 2019, Pages 1447 – 1461

[2] Saptarshi Debroy, Priyanka Samanta, Amina Bashir, Mainak Chatterjee, “SpEED-IoT: Spectrum aware energy efficient routing for device-to-device IoT communication”, Future Generation Computer Systems, Elsevier, Volume 93, April 2019, Pages 833-848

[3] Gaofei Sun, Xiaoshuang Xing and Xiangping Qin, “Energy harvesting-based data uploading for Internet of Things”, EURASIP Journal on Wireless Communications and Networking, Springer, Volume 153, 2019, Pages 1-13

[4] Beytullah Yigita, Gurkan Gur, Fatih Alagoz and Bernhard Tellenbach, “Cost-Aware Securing of IoT Systems Using Attack Graphs”, Ad Hoc Networks, Elsevier, Volume 86, April 2019, Pages 23-35

[5] Neha K. Nawandar and Vishal R. Satpute, “IoT based low cost and intelligent module for smart irrigation system”, Computers and Electronics in Agriculture, Elsevier, Volume 162, 2019, Pages 979–990

[6] Hongyang Yan, Yu Wang, Chunfu Jia, Jin Li, Yang Xiang and Witold Pedrycz, “IoT-FBAC: Function-based access control scheme using identity-based encryption in IoT”, Future Generation Computer Systems, Elsevier, Volume 95, June 2019, Pages 344-353

[7] Bingxian Lu, Lei Wang, Jialin Liu, Wei Zhou, Linlin Guo, Myeong-Hun Jeong, Shaowen Wang, Guangjie Han, “LaSa: Location Aware Wireless Security Access Control for IoT Systems”, Mobile Networks and Applications, Volume 24, Issue 3, June 2019, Pages 748–760

[8] Fei Li, Yogachandran Rahulamathavan, Mauro Conti and Muttukrishnan Rajarajan, “Robust access control framework for mobile cloud computing network”, Computer Communications, Elsevier, Volume 68, 1 September 2015, Pages 61-72

[9] Yi Liu, Yinghui Zhang, Jie Ling and Zhusong Liu, “Secure and fine-grained access control on e-healthcare records in mobile cloud computing”, Future Generation Computer Systems, Elsevier, Volume 78, Part 3, January 2018, Pages 1020-1026

[10] Alessandro Biason, Chiara Pielli, Andrea Zanella, and Michele Zorzi, “Access Control for IoT Nodes with Energy and

Fidelity Constraints”, IEEE Transactions on Wireless Communications, Volume 17, Issue 5, May 2018, Pages 3242 – 3257