JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Review of Energy Efficiency in Security of 5G Internet of Things (IoT) Applications

[1]Sweta Verma, [2]Dr. Nikita Shivhare Mitra
[1]M.Tech Scholar, [2]Associate Professor,
[1&2]Department of Electronics and Communication Engineering,
[1&2]Oriental Institute of Science & Technology, Bhopal, India

Abstract : 5G will be quickly become the new standard for cellular networks. The Internet of Things (IoT) is rapidly developing and expanding. 5G will increase cellular bandwidth by huge amounts, making it much easier for the Internet of Things to network large numbers of devices together. 5G will be 10 times faster than current LTE networks. This increase in speed will allow IoT devices to communicate and share data faster than ever. The security is a major concern of digital communication, as the technology enhances the security concern is also enhancing to meet the requirement of the 5G-IOT communication. This paper includes the energy efficiency of the nodes in security for 5G-IOT applications.

***IndexTerms* - Energy, IoT, Security, 5G, Efficiency, Latency, Security, Wireless.**

I. INTRODUCTION

Security services are typically provided by applying schemes such as encryption/decryption and signature/ verification. These schemes are generally designed to maintain a high level of security against attacks, and are known to be resource-intensive. In the other hand, when considering the IoT, many connected devices are resource-constrained. Objects, such as sensors and RFID tags, can be limited in terms of energy, memory, computation, and storage. In addition, as such devices can be battery-powered and expected to operate for a long time, energy consumption is very critical for the IoT. Heavy security could lower the lifetime of IoT services and deviate the objects from their main tasks. Therefore, security services must be adapted to meet the energy-constrained nature of the IoT, while considering the 5G architecture. The challenging problem of energy efficiency in security of the Internet of Things (IoT) is tackled in this article. The authors consider the upcoming generation of mobile networks, 5G, as communication architecture for the IoT. The concept of adaptive security is adopted, which is based on adjusting the security level as per the changing context. It has the potential of reducing energy consumption by adapting security rather than always considering the worst case, which is energy consuming. The consideration of 5G introduces new dynamics that can be exploited to perform more adaptation [1].

Figure 1: 5G-IOT System

Evolution of mobile networks have fulfilled the increasing demands for enhanced performance, availability, portability, elasticity, and energy efficiency posed by the ever growing network services. In line with the progression, 5G depicts the next generation of mobile networks that further promises remarkable performance improvements as well as creation of new value chain. In parallel to 5G, the Internet of Things (IoT) has emerged as another new paradigm for interconnection of massive communication-capable heterogeneous smart objects. 5G is envisaged to broaden IoT's scope and fields of applicability. However, since current mobile networks and also more general IoT systems are based on centralized models thus it is anticipated that they will face tremendous challenges to meet-up the requirements of future 5G-enabled-IoT use cases [2].

The main advantages of this paradigm are core network offloading and low latency for delay-sensitive applications (e.g., automatic control). We have reviewed the state-of-the-art in the PEC paradigm and its applications to the IIoT domain, which have been enabled by the recent developments in 5G technology. We have classified and described three important research areas related to PEC-distributed artificial intelligence methods, energy efficiency, and cyber security. We have also identified the main open challenges that must be solved to have a scalable PEC-based IIoT network that operates efficiently under different conditions. By explaining the applications, challenges, and opportunities, our work reinforces the perspective that the PEC paradigm is an extremely suitable and important deployment model for industrial communication networks, considering the modern trend toward private industrial 5G networks with local operations and flexible management [3].

The commercialization of 5G has greatly promoted the development of medical Internet of Things (IoT). More medical devices connected to the Internet may further increase the communication power consumption. Meanwhile, privacy protection technique in cloud computing cannot match the rapid development of medical applications. Therefore, exploring secure, balanced and energy-efficient data transmission between medical devices and cloud servers is extremely challenging. We build a secure energy-saving communication and encrypted storage model by adding secure energy-saving communication scheme and encryption algorithm to the traditional medical cloud model. Specifically, we propose a communication authentication algorithm MedGreen based on elliptic curve and bilinear pair [4].

The purpose of the first phase is to decode information, and energy harvesting (EH) is performed in accordance with the TSPS protocol. The purpose of the second phase is to transmit information to multiple destinations using the amplify-and-forward (AF) technique. In this study, we introduce a multirelay cooperative scheme (MRCS) to improve the secrecy performance. We derive analytical expressions for the secrecy outage probability (SOP) of the MRCS and that of the noncooperative relay scheme (NCRS) by using the statistical characteristics of the signal-to-noise ratio (SNR). Specifically, we propose an optimal relay selection scheme to guarantee the security of the system for the MRCS. In addition, Monte Carlo simulation results are presented to confirm the accuracy of our analysis based on simulations of the secrecy performance under various system parameters, such as the positions and number of ERs, the EH time, and the EH efficiency coefficients. Finally, the simulation results show that the secrecy performance of our MRCS is higher than that of the NCRS and the traditional cooperative relay scheme (TCRS) [6]. To further enhance the energy efficiency (EE) performance of fifth generation (5G) Internet of Things systems, an integrated structure is proposed in this work. That is, other than prior studies that separately study the wireless and wired parts, the wireless and wired parts are holistically combined together to comprehensively optimize the EE of the whole system [9].

II. LITERATURE SURVEY

H. Hellaoui, et al.,[1] presents solution introduces an intelligence in the application of security, from the establishment phase to the use phase (end-to-end). The security level related to the used cryptographic algorithm/key is adapted for each node during the establishment phase, so to match with the duration of the provided services. A new strategy is formulated that considers both IoT and 5G characteristics. In addition, a solution based on the framework of the coalitional game is proposed in order to associate the deployed objects with the optimized security levels. Moreover, the application of security is also adapted during the use phase according to the threat level. Trust management is used to evaluate the threat level among the network nodes, while existing works focus on performing the adaptation during the use phase.

T. M. Hewa et al.,[2] solve inevitable issues Blockchain stands out as promising technology. Some of the offerings of Blockchain technology are immutability, non-repudiation, proof of provenance, integrity, privacy, etc. Blockchain's combination with 5G and IoT still requires essential insights with respect to concrete application domains, scalability, privacy issues, performance, and potential financial benefits. The work aims to elaborate and emphasize the key aspects of the use of Blockchain for 5G and IoT.

A. Narayanan et al.,[3] This article surveys emerging technologies related to pervasive edge computing (PEC) for industrial internet-of-things (IIoT) enabled by fifth-generation (5G) and beyond communication networks. PEC encompasses all devices that are capable of performing computational tasks locally, including those at the edge of the core network (edge servers co-located with 5G base stations) and in the radio access network (sensors, actuators, etc.).

J. Zhang et al.,[4] In the algorithm, the two communication parties can complete the key establishment and identity authentication only after one communication, which effectively balances the resource overhead of the key center and the user, and resists the Man-in-the-middle attack. Aiming at the characteristics of large repetition and high sensitivity of medical data, we present a secure data storage algorithm MedSecrecy based on Huffman compression and RC4. The algorithm not only maintains the RC4 encryption efficiency, reduces the amount of cipher text data, but also improves confidentiality, randomness and security of the key stream. Comprehensive analysis and simulations show that our system is secure, energy-saving and highly efficient for EHR.

M. Poongodi et al.,[5] presents the efficiency of the proposed method, various network parameters are considered such as Packet Delivery Ratio (PDR), Average Latency (AL), Detection Rate (DR) and Energy Consumption (EC). In the proposed research work, the metric PDR is used to know successful delivery of data packets to the destination vehicle without any interrruption. These parameters are used to measure how effectively the data is delivered to the destination from source vehicle.

A. Nguyen et al.,[6] investigate the physical layer security (PLS) of a wireless sensor network (WSN) that consists of a base station (BS), multiple sensor nodes (SNs), and multiple energy-limited relays (ERs) in the presence of a passive eavesdropper (EAV). We adopt a time-switching/power-splitting (TSPS) mechanism for information transmission. The communication protocol is divided into two phases.

A. Ahad, et al.,[7] cases such as remote surgeries and Tactile Internet will spur the need for Ultra Reliability and Low Latency Communications or Critical Machine Type Communication. The existing communication technologies are unable to fulfill the complex and dynamic need that is put on the communication networks by the diverse smart healthcare applications. Therefore, the emerging 5G network is expected to support smart healthcare applications, which can fulfill most of the requirements such as ultra-low latency, high bandwidth, ultra-high reliability, high density, and high energy efficiency.

Ovidiu et al.,[8] The IoT and Industrial Internet of Things (IIoT) are evolving towards the next generation of Tactile IoT/IIoT, bringing together hyperconnectivity (5G and beyond), edge computing, Distributed Ledger Technologies (DLTs), virtual/ andaugmented reality (VR/AR), and artificial intelligence (AI) transformation. Following the wider adoption of consumer IoT, the next generation of IoT/IIoT innovation for business is driven by industries, addressing interoperability issues and providing new end-to-end security solutions to face continuous treats.

D. Zhang et al.,[9] The integrated system structure is introduced beforehand with the proposed unified control center components for better deployment of the select-and-sleep mechanism. In addition, in the wireless part, one cellular partition zooming (CPZ) mechanism is proposed. In contrast, in the wired part, a precaching mechanism is introduced. With these proposals, the proposed system EE performance is investigated. Comprehensive computer-based simulation results demonstrate that the proposed schemes display better EE performance.

Jong Hyuk et al.,[10] The works in this special section focuses on computational intelligence for communication and sensing systems. As billions of phones, appliances, drones, traffic lights, security systems, environmental sensors, radars, and other radio-connected sensing and communication devices sum into a rapidly growing Internet of Things (IoT), many challenges such as spectrum allocation and efficiency, energy efficiency, security, have emerged as urgent topics to be solved. For example, 5G wireless communications will be deployed in the 28 GHz, 37 GHz, 39GHzfrequency band, which may co-exist with radars and other sensing devices.

J. H. Park et al.,[11] The MEC supports IoT devices to improve their efficiency and scalability; helps to reduce latency delay for real-time applications, bandwidth bottlenecks, and energy consumption; and delivers contextual information processing. MEC offers many features and capabilities, such as access to a multitude of network interface (from 4G and 5G to Wi-Fi), support for device mobility, device context, geo-location awareness, and geographical distribution. Such attributes can support the real-time processing requirements of the Internet of Everything application, such as patient care, disaster management and detection (e.g., earthquakes), and flood monitoring.

E. Hossain et al.,[12] presents a comprehensive survey of CB schemes for traditional wireless networks such as cellular networks, wireless local area networks and wireless sensor networks, and then provides a detailed discussion on the CB schemes proposed for cognitive radio networks. Finally, the work highlights a number of issues and challenges regarding CB in cognitive radio sensor networks and also provides some guidelines on using CB schemes in these futuristic networks.

III. DIFFERENT SECURITY APPROACHES

A. Privacy preserving

Privacy preservation in data mining is an important concept, because when the data is transferred or communicated between different parties then it's compulsory to provide security to that data so that other parties do not know what data is communicated between original parties. Preserving in data mining means hiding output knowledge of data mining by using several methods when this output data is valuable and private. Mainly two techniques are used for this one is Input privacy in which data is manipulated by using different techniques and other one is the output privacy in which data is altered in order to hide the rules.

B. ID Cryptography

Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key. The public string could include an email address, domain name, or a physical IP address. This approach allowed users to verify digital signatures using only public information such as the user's identifier. Under Shamir's scheme, a trusted third party would deliver the private key to the user after verification of the user's identity, with verification essentially the same as that required for issuing a certificate in a typical PKI.

C. Ad-Dissemination

Dissemination takes on the theory of the traditional view of communication, which involves a sender and receiver. The traditional communication view point is broken down into a sender sending information, and receiver collecting the information processing it and sending information back, like a telephone line.

D. Token Based

Token-based confirmation plans, for example, Pledge 2 and OpenID Interface Combined Validation give helpful options in contrast to shared insider facts and testaments, and furthermore take into consideration the presentation of far reaching strategy controls connected to IoT get to necessities. Testament based confirmation in examination with shared mystery validation is progressively useful with vast number of gadgets, on the grounds that the overhead about dealing with the insider facts ends up huge for countless. Testament based verification utilizes deviated calculations and manages the handling of authentications

C. Frame-work

While the broadly useful key trades are security arrangements at the Web space, TCP/IP security conventions are one of the essential parts of structuring IP-based IoT security arrangements. Numerous conventions, for example, IKEv2/IPsec, TLS/SSL, DTLS, HIP, PANA, and EAP are conceivable arrangements in the 6LoWPAN and Center IETF working gatherings to give a progressively secure IoT information transmission

Table 1: Comparison of different security algorithm

Parameter	Privacy Preserving	ID Cryptography	Ad-Dissemination	Token	Frame-Work
Complexity	Less	High	Average	Very less	High
Buffer Size	Less	More	Average	Very High	Average
Through put	High	Average	Average	Very less	High
Cost	High	Very less	Medium	Less	Less
Time	Medium	Less	Medium	Very High	Very less
Range	10 km	1-2 km	5 km	10 km	1-2 km

IV. CONCLUSION

However, 5G brings a range of benefits to the IoT which are not available with 4G or other technologies. These include 5G's ability to support a massive number of static and mobile IoT devices, which have a diverse range of speed, bandwidth and quality of service requirements. IoT devices include wireless sensors, software, actuators, and computer devices. They are attached to a particular object that operates through the internet, enabling the transfer of data among objects or people automatically without human intervention. This paper review of the various aspects including energy efficiency in security of 5G internet of things (IoT) applications.

REFERENCES

1. H. Hellaoui, M. Koudil and A. Bouabdallah, "Energy Efficiency in Security of 5G-Based IoT: An End-to-End Adaptive Approach," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6589-6602, July 2020, doi: 10.1109/JIOT.2020.2974618.
2. T. M. Hewa, A. Kalla, A. Nag, M. E. Ylianttila and M. Liyanage, "Blockchain for 5G and IoT: Opportunities and Challenges," 2020 IEEE Eighth International Conference on Communications and Networking (ComNet), 2020, pp. 1-8, doi: 10.1109/ComNet47917.2020.9306082.
3. A. Narayanan et al., "Key Advances in Pervasive Edge Computing for Industrial Internet of Things in 5G and Beyond," in IEEE Access, vol. 8, pp. 206734-206754, 2020, doi: 10.1109/ACCESS.2020.3037717.
4. J. Zhang, H. Liu and L. Ni, "A Secure Energy-Saving Communication and Encrypted Storage Model Based on RC4 for EHR," in IEEE Access, vol. 8, pp. 38995-39012, 2020, doi: 10.1109/ACCESS.2020.2975208.
5. M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi and M. Ma, "Intrusion Prevention System for DDoS Attack on VANET With reCAPTCHA Controller Using Information Based Metrics," in IEEE Access, vol. 7, pp. 158481-158491, 2019, doi: 10.1109/ACCESS.2019.2945682.
6. A. Nguyen, V. Nhan Vo, C. So-In, D. Ha, S. Sanguanpong and Z. A. Baig, "On Secure Wireless Sensor Networks With Cooperative Energy Harvesting Relaying," in IEEE Access, vol. 7, pp. 139212-139225, 2019, doi: 10.1109/ACCESS.2019.2941915.
7. A. Ahad, M. Tahir and K. -L. A. Yau, "5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions," in IEEE Access, vol. 7, pp. 100747-100762, 2019, doi: 10.1109/ACCESS.2019.2930628.
8. Ovidiu Vermesan; Joëel Bacquet "End-to-end Security and Privacy by Design for AHA-IoT Applications and Services," in Next Generation Internet of Things Distributed Intelligence at the Edge and Human Machine-to-Machine Cooperation , River Publishers, 2018, pp.103-138.
9. D. Zhang, Z. Zhou, S. Mumtaz, J. Rodriguez and T. Sato, "One Integrated Energy Efficiency Proposal for 5G IoT Communications," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 1346-1354, Dec. 2016, doi: 10.1109/JIOT.2016.2599852.
10. Jong Hyuk Park; Vincenzo Piuri; Hsiao-Hwa Chen; Yi Pan "Special Issue on Computational Intelligence for Communications and Sensing," in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 4, no. 1, pp. 1-4, Feb. 2020, doi: 10.1109/TETCI.2019.2963469.
11. J. H. Park, V. Piuri, H. Chen and Y. Pan, "Guest Editorial Special Issue on Advanced Computational Technologies in Mobile Edge Computing for the Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4742-4743, June 2019, doi: 10.1109/JIOT.2019.2921237.
12. E. Hossain, "Editorial: Second Quarter 2016 IEEE Communications Surveys and Tutorials," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 899-904, Secondquarter 2016, doi: 10.1109/COMST.2016.2559959.