Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 04
Pages: 181-187
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.4.002

Optimal Key Handover Management for Enhancing Security in Mobile Network

Dr. V. Suma
Professor,
Department of Information Science & Engineering,
Dayananda Sagar College of Engineering,
Bangalore, India.

Dr. Wang Haoxiang
Professor,
Go Perception Laboratory,
Cornell University,
USA.

Abstract: - The 3GPP long term Evolution or System Architecture Evolution (LTE/SAE) was designed for the dispositioning of the mobile networks towards 4G. The significant hurdle of 4G is about cementing the privacy and security gap. Due to the disclosures in the connectivity of public networks, a single malicious device could jeopardize the operation of a whole network of devices. The key deliverance handling within the 3GPP LTE/SAE is developed to unauthorize the keys that are being attacked and, in result, to alienate the miscreant keys off the chain of network. The proposed article recognizes the attacks that jeopardize the safe connectivity among the stops in the network chain and details the vulnerability of the key deliverance administration to desynchronization attacks. Even though the periodic upgrade of the root could prove to be a fundamental part of the system, the work proposed brings an emphasis on reducing the impact of desynchronization attacks which currently are unable to be prevented efficiently. The main focus of the design is to shed light on the ways the network operators work to confirm the optimal intervals for the periodic updates to reduce the signal weightage while providing secure user mobility. The analysis and model simulations intend to disclose the influence of the period of root key upgrade on integral operational levels such as constellation and user experience.

Index terms *– Validation and key correspondence, Evolved Packet System (EPS), Key deliverance handling, Bees Algorithm, LTE security*

1. INTRODUCTION

Owing to the onset in the information and communication technology there was a recent increase in the cellular data usage and a need for new application drive which motivated the shift of 3GPP into the fourth generation [1]. The programmers of the 3GPP Long Term Evolution or System Architecture Evolution (LTE/SAE) system have predicted the genesis of the Evolved Packet System (EPS) to mark the shift of 3GPP into the fourth generation. The improved access network of the EPS reinforced the radionics-oriented devices of the 3GPP cellular connectivity, offering higher data rate with much less deferral rate. The EPS was developed to suit the needs of flat Internet Protocol (IP) connectivity and the interworks with various heterogeneous radionics-oriented connections and services.

These structural aspects of the design are focused to bring out the attributes of LTE/SAE systems to the forefront. The flat all-IP architecture equips all of the radionics-oriented protocols to surcease in a single node called evolved NodeB, henceforth eNodeB. The constituents of the eNodeB within the Universal Mobile Telecommunications System (UMTS) are comprised of a NodeB and a Radio Network Controller (RNC). With the eNode located in a disregarded region, the positioning of the network protocols of radionics-oriented connectivity in the eNodeB makes them pervious towards unverified network accesses [2]. The communication of the Internet with various multiple radionics-oriented networks lays bare the susceptibility of these networks to security breaches from an outsider and, eventually, brings fatal consequences to LTE security.

The uniqueness of the characteristics in the design of LTE/SAE influenced various attributes of the safety measures in the EPS connectivity. The key management handovers and the reduction of the involved security risks,

ISSN: 2582-4104
Submitted: 06.12.2020
Accepted: 29.12.2020
Published: 05.01.2021

among the other features, are the focal points of this article. The fundamental risk of key deliverance handling is that the breach might jeopardize the term keys in the source [3]. Generally, the key deliverance handling lessens the risk through a partition of keys in the deliverance among the operators of the root. The partition of keys manages the security breaches through a process of localization, which segregates the jeopardized key in a root operation from jeopardizing the keys of other base stations.

The preparations of deliverance in LTE/SAE do not consist of the source network due to the reasons of efficient operation. There is a transmission of term key from the root eNodeB towards the eNodeB in the target succeeding the deliverance. The source network is never obligated to sustain a mode of Individual User Equipment (UE). The model permits the deliverance of an unmodified term key that allows the eNodeB in the target to recognize the term key used by the eNodeB in the source [4]. There is a computation of a different term key by the eNodeB in the root with the applied one-way function on the old term key. It prevents pre-mentioned operation by ensuring a rearward key-segregation during the deliverance. Nonetheless, the rearward key-segregation only could stop an eNodeB from restoring the old term keys through the term key that is being used [5]. The eNodeB would be aware of all the term keys employed in the other mobilizations in the network of deliverances, otherwise. Consequently, the leading key mobilizations were designed to safeguard the addition of new sources to the method of building a different term key for the subsequent sitting.

Under certain circumstances, as it could be demonstrated, the key deliverance handling fails in ensuring the segregation of the leading key during the attack by an alteration of a rogue root operator, known by the name desynchronization attack. The maintenance of the intactness of the key of deliverance by eNodeB is hindered by a desynchronization attack [6]. This sort of susceptibility in synchronization is plausibly disruptive in the key deliverance handling which may prove a pathway for the verminous adversaries to compromise the keys between users and the eNodeBs.

This attack is likely to continue until the next root update in which the materials of the handover key need to be built from square one rather than being an inflexion of the old term key. Only through such a process the calamitous effect of the compromised keys could be contained [7]. Instead of encircling around the technicalities that surround a definite fix that could protect the desynchronization attacks, the most operational remedy would be the periodical refreshing of the root key [8]. The creation of short-term root keys appears to be the intuitive counter-reaction to reduce the impacts of the compromising keys. Nevertheless, the frequency of the refreshing and the signal weightage in the root upgrade make it not an optimal operational choice. However, the longer period of root update makes them vulnerable to desynchronization attacks as well.

The major issue for the administrators and the network services would be about choosing the most efficient period of root upgrade with the highest rate of correspondence between the signal weightage and the level of disclosure of data pack vulnerability to risks due to the jeopardized key deliverance [9]. The dependency of the issue on time and space hinders the existence of neither a universally accepted period of root upgrade nor acceptable alignments which can be appropriated to different circumstances. With an emerging rate of security risks, the paper tends to explicate the formulation of a universal root upgrade period measure to suit different junctures of time and space. On the primary level, the formulation of the acceptable tradeoff value, the timings of the key deliverance handling have been given in diagrams based on the period of root upgrade to compute the times of activity of the jeopardized key [10]. The study was furthered by the model algorithm to estimate the value of the times of operability of the jeopardized key and to signify the anticipated estimates of the signal weightage and the disclosed data packs during the activities [11]. Through this model, the period of root upgrade can be appropriated based on the demands of the service providers and administrators. The intention of formulating an optimal interval value is to reduce the required signal weightage for root upgrade while restraining the vulnerability of data packets to the jeopardized key.

This Study’s investigation runs three ways: (1) Identification of the errancy of the key deliverance handling of the EPS networks;(2) Formulation of the optimal algorithm for the EPS key deliverance handling to compute the estimate of the impacts of a jeopardized key; (3) to study the operational levels, such as the user network movement, the terrain and so on, in the selection of a favourable spot for root key upgrade [12]. The comprehensive outputs of these simulations authenticate the algorithm and, moreover, explicate those practical facets of the optimal key [13]. The remaining parts of the article are structured in the following manner. Sec. 2 of this paper provides a synopsis of

ISSN: 2582-4104
Submitted: 06.12.2020
Accepted: 29.12.2020
Published: 05.01.2021

the EPS system of Security expounding the details of the key deliverance handling. Sec. 3 elucidates about those aberrancies in the safety of key deliverance handling. Sec. 4 brings the model algorithm to study the vulnerability towards a jeopardized key and to formulate the value of the alignment amidst the signal weightage and the number of the jeopardized data packets while the deliverance of the key is operational. Sec. 5 tests the credibility of the value derived through the algorithm and assimilates factual outputs with the practical effectiveness of the algorithm. Sec. 6 represents issues of management and implication with administrators and service providers. Sec. 7 presents a literature review related to the network security of 4G and the arithmetic procedures of 3GPP security system, prior to the summing up in Sec. 8.

2. OPTIMAL HANDOVER MANAGEMENT

The primary intention of the 3GPP LTE system is secure connectivity with high data process for 4G network. Despite the upgraded safety designs of 4G, there still are some gaps and vulnerabilities which could welcome several variants of cyber-attacks. The paper deals with one such attack known as desynchronization attack in 3GPP key deliverance and handling. During the operation due to a miscreant root irruption, a desynchronization attacker finds the vulnerability to compromise the 3GPP system [14]. The article demonstrates how it also leads to the jeopardy of the communication through the 4G network and proposes a remedy for overcoming such attacks. The proposed model explores the ways in which the administrators could compute the favourable root upgrade period to lessen signal weightage and avoid risks in the security of the mobility of the user data. The prediction of an optimal period of the key upgrade is done using an Improved Artificial Bee Colony (IABC) algorithm. On the first step towards formulating an acceptable alignment, the key deliverance handling timings have been diagramed based on the period of root key upgrade to measure the value of the period during which the jeopardized component was active [15]. Later, the model algorithm was investigated to calculate the estimated period of activity of the jeopardized key and to signify the estimated number of the signal weightage and the amount of the vulnerability of data packs. Through this methodology, the period of root upgrade can be appropriated as the administrators require. The intention of formulating an optimal period value is to reduce the required signal weightage for root upgrade while restraining the data packets susceptibility to the jeopardized key. The results of examinations and experiments show that the proposed model demonstrated a better result compared to extant algorithms.

2.1. Process of the proposed scheme

The investigation of the study runs three ways: (1) Identification of the errancy of the key deliverance in the EPS system;(2) Formulation of the optimal algorithm for the key deliverance in the EPS to calculate the estimation of the impact of a key that is being attacked; (3) to examine the operational levels, such as use network movement, terrain and so on, in the selection of a key upgrade period using IABC algorithm for root upgrades [16]. The comprehensive results of the simulations authenticate the model and explicate the practical facet of the algorithm.

2.2. Bee’s basic behaviour

The Bees Swarm Intelligence Algorithm is an extensive stream of computer science dedicated to design algorithms and to study the efficient computational methods for problem-solving animated through the ingenious collective performance of the bee colonies. This design is proposed by Tereshko based on the foraging behaviour of the honeybee colonies [17]. The model elucidates on the collective and cooperative intelligence of the honeybee drones, which essentially consists of three constituents: energy supply employed foragers and unexercised pillagers. As elaborated by Tereshko,

(i) Energy supply: The selection of an energy supply begins with the forager bee’s evaluation of the properties of the food source, such as the proximity of the hive with the food source, abundancy of the energy, the sapidity of the nectar, and the level of difficulty involved in extracting this energy. These parameters are used as the signifiers of the quality of the food source.

(ii) Employed foragers: An employed forager bee works in a specifically assigned location of a food source. It brings a set of information from the location to the other drones lodging in the colony. The information consists of the trajectory of the food source, the waggle dance direction, the distance from the hive and the rating of quality or, preferentially, fitness.

ISSN: 2582-4104
Submitted: 06.12.2020
Accepted: 29.12.2020
Published: 05.01.2021

(iii) Unexercised pillager: An unexercised pillager drone is a bee that is set out to look for a food source to extract the energy. This Pillager bee could either be searching the environment for a random food source or be locating a specific source based on the

(iv) information on hand given by an employed forager drone. The average amount of scouts in a hive would be around 5–10%.

The Bee Swarm Intelligence is an extensive conception of technology that incorporates the natural system as well as artificial systems and provides an ingenious way for finding collective optimal solutions [18]. The recent decades have witnessed a gradual increase in the appropriation of this model in problem-solving issues.

2.3. Key Management Through an Improved Artificial Bee Colony

The efficiency of the Bee Swarm Intelligence involves its dealing with both natural and artificial systems. The concept of collective and cooperative intelligence of the system proved to be an effective way of problem-solving. Researchers around the world, in recent decades, have been utilizing this model in various issues that surround various fields. This model, in networking, is appropriated to find solutions to security issues by optimizing the path, aggregation, security and so on. The proposed model uses it for a favourable articulation in administering the keys [19]. A fitting algorithm to appropriate the root upgrade would be the preference of the network administrators due to the security risks that encircle a 3GPP system. An unnecessarily frequent root upgrade would mean signal overweight, whereas a debilitated infrequent upgrade of the root might expose the privacy of the users and cause security risks from external threats. The discussion of this article sets out, given these parameters, to find the optimal point of operation for upgrading the root to reduce the susceptibility of data packs and the signal weightage.

An optimal value generally would lie amidst two of the definitive values that correspond to each other inversely. The optimal value is defined as the one with the range of T_u, in which the network operators would be able to manage an acquiescence among signal weightage and security risks [20]. The optimal range of T_u would bring the E[N] and E[S] to their possibly least value. Nevertheless, a universally accepted value of T_u could not exist due to the difference in value determined by the network operators and management policies. Hence, this model intends to bestow the administrators with a choice in distributing variant values to E[N] and E[S] following the management policies to bring T_u to its optimal value [21]. While E[N] is classified as the appraised amount of user data vulnerability, E[S] is defined as the estimated rate of signal weightage.

An Improved Artificial Bee Colony Algorithm processes in the following way:

1. The E [S] and E [N] values are established for the U-plane data the AS packets contain and RRC signals that are susceptible to eavesdropping.
2. Compute the corresponding placement of the nodes and Time Distance ($_{ui,\ tj}$) Function: RF = √ (u (n-1) i-$u_{ni})^2$ + (t(n-1) $_j$ – t_{nj})2 + (R_f – R_i), in which RF stands for a contingent placement of the distance function, β denotes the retributive value of the collision with the immobile object and announces the value of profiles.
3. Generate the neighbourhood the fitness value of each of the search computed utilizing the equation: fitness i= 1/F_j, wherein j signifies the profiles of the neighbourhood whose fitness value needs to be derived.
4. The employed forager bees are deployed to improve or modify the neighbourhood searches inconstantly.
5. The neighbourhood profiles that are unable to be modified of their fitness value are considered forsaken.
6. Likewise, the neighbour profile with the optimal value would be updated and improved.
7. Figure out the Relative position of User and Time Distance Function of the profiles from the neighbourhood with a consideration of the collision but with dynamic objects this time, adapting the equation: $RF_{d\ =}$ F + γ, wherein γ signifies the retributive value of the collision with dynamic profiles and j denotes the number of dynamic profiles in the collision.
8. The profiles, including dynamic profiles, need to be organized in a descending order based on their fitness value.

ISSN: 2582-4104
Submitted: 06.12.2020
Accepted: 29.12.2020
Published: 05.01.2021

9. The profile with the optimal fitness value is expected to be appropriated on the bystanding bees for further modifications.
10. When a specific profile is unable to be improved after a certain number of trials, it is considered forsaken.
11. The employed foragers of the forsaken profile becomes a scout and seeks for other profiles with preferable fitness value.
12. The process would be exacted to several fixed cycles to improve the fitness of the profiles.
13. The triangle inequality method to could be applied in further optimizations of the key management for improved results.

Following the abovementioned steps, the optimal root key can be updated. Apart from the intonation on the preventive measures, the significance of the model rests on its ability to reduce the impact of desynchronization attacks and key compromises by unknown parties. The proposed model reduces the energy cost for good.

3. SIMULATION RESULT AND ANALYSIS

Figure.1 depicts the clusters the of cells. Each of the cells would be attached on the basis of the shortest path trajectory. A100 random cells have been selected wherein the 14th cell is held as the current cell to which the mobile station is associated and the user is supposed to move towards the 36th cell through the nodes in-between the numbers 17, 1 and 56.

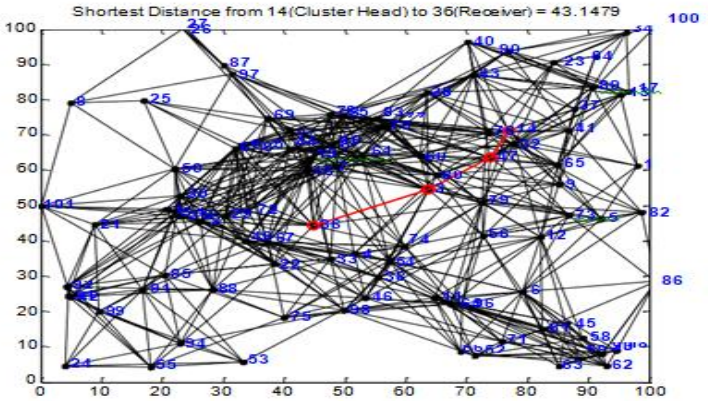

Figure: 1 Cells connected based on shortest path vector

Figure.2 represents the distribution of keys from each of the cells when a mobile user enters a different cell. Figure.2 (a) expounds the encryption of the mobile user through the key 40.9896 at cell number 14.

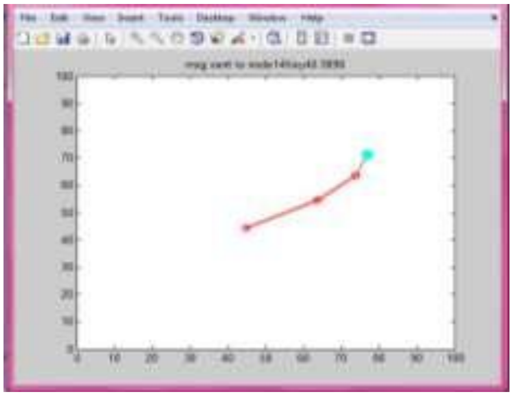
File Edit View Insert Tools Desktop Window Help
msg sent to node14Key40.9896
100
90
80
70
60
50
40
30
20
10
0
0
10
20
30
40
50
60
70
80
90
100

Figure: 2(a)

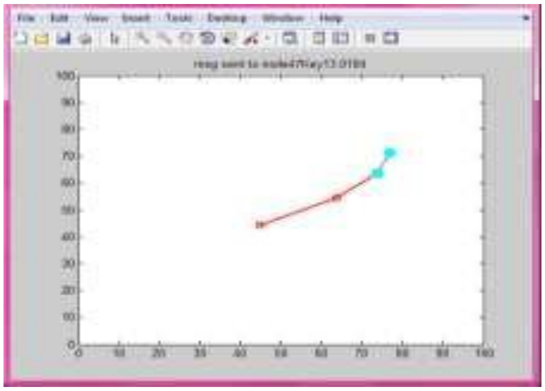
File Edit View Insert Tools Desktop Window Help
msg sent to node47Key13.0189
100
90
80
70
60
50
40
30
20
10
0
0
10
20
30
40
50
60
70
80
90
100

Figure: 2(b)

ISSN: 2582-4104
Submitted: 06.12.2020
Accepted: 29.12.2020
Published: 05.01.2021

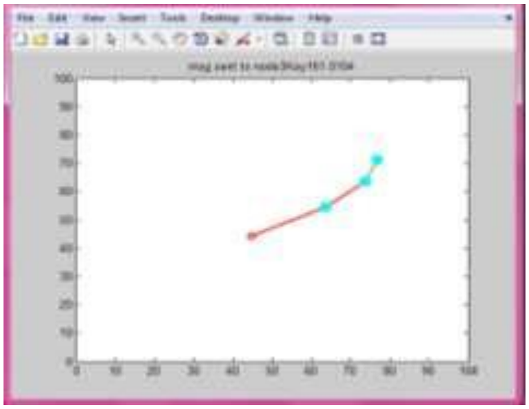

Figure: 2(c)

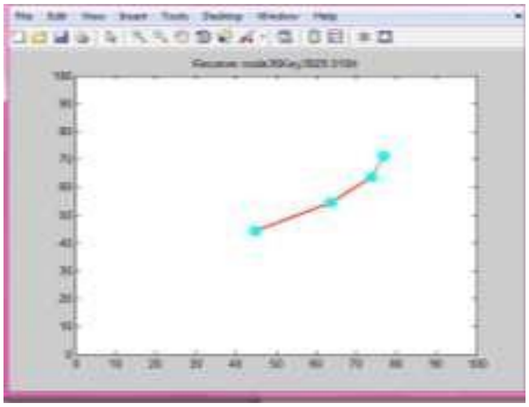

Figure: 2(d)

The key will be updated upon the user's reach in the 36th cell to 3829.0104, shown in the figure2 (d). Figure 2 (b) and (c) show the encrypted key updates upon the mobile user's movement across the nodes. Therefore, the proposed model reinstates the security of the user data even when they move across different cells.

4. CONCLUSION

The segregation of leading keys in the 3GPP LTE/SAE technology is likely to get compromised due to the miscreant root irruption. Though it has been said that the periodical updating of the root key reduces the level of risk, the selection and appropriation of the optimal key could be an issue with ill-equipped solutions due to the difficulty faced in balancing the signal weightage and the level of vulnerability of data packs. The developed algorithm equips the network operators in selecting and appropriating an optimal value of the upgrade period of the keys that best suits their web management policies.

REFERENCES

[1] Ahmed, A. A., & Alzahrani, A. A. (2019). A comprehensive survey on handover management for vehicular ad hoc network based on 5G mobile networks technology. *Transactions on Emerging Telecommunications Technologies*, *30*(3), e3546.

[2] Gódor, G., Jakó, Z., Knapp, Á., & Imre, S. (2015). A survey of handover management in LTE-based multi-tier femtocell networks: Requirements, challenges and solutions. *Computer Networks*, *76*, 17-41.

[3] Haldorai, A., & Ramu, A. (2020). Security and channel noise management in cognitive radio networks. *Computers & Electrical Engineering*, *87*, 106784.

[4] Han, C. K., & Choi, H. K. (2012). Security analysis of handover key management in 4G LTE/SAE networks. *IEEE Transactions on Mobile Computing*, *13*(2), 457-468.

[5] Kalyani, G., & Chaudhari, S. (2020). An efficient approach for enhancing security in internet of things using the optimum authentication key. *International Journal of Computers and Applications*, *42*(3), 306-314.

[6] Kaur, R., & Mittal, S. (2020). SINR and Fuzzy Approach based Enhanced Handoff Decision Making Algorithm. *Available at SSRN 3565899*.

[7] Kim, S., & Park, B. (2019). Multi-routing based Mobility Management with an Optimized Security Network. *IEIE Transactions on Smart Processing & Computing*, *8*(4), 290-297.

[8] Krishna Jyothi, K., & Chaudhari, S. (2019). A secure cluster-based authentication and key management protocol for machine-type communication in the LTE network. *International Journal of Computers and Applications*, 1-11.

[9] Kumar, S., & Gaur, M. S. (2019, July). Handoff Prioritization to Manage Call Admission Control in Mobile Multimedia Networks for Healthcare. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-7). IEEE.

[10] Liu, L., Chen, C., Pei, Q., Maharjan, S., & Zhang, Y. (2020). Vehicular edge computing and networking: A survey. *Mobile Networks and Applications*, 1-24.

ISSN: 2582-4104
Submitted: 06.12.2020
Accepted: 29.12.2020
Published: 05.01.2021

[11] Liyanage, M., Ahmed, I., Okwuibe, J., Ylianttila, M., Kabir, H., Santos, J. L., ... & De Oca, E. M. (2017). Enhancing security of software defined mobile networks. *IEEE Access*, *5*, 9422-9438.

[12] Manjula, T., & Anand, B. (2019). A secured multiplicative Diffie Hellman key exchange routing approach for mobile ad hoc network. *Journal of Ambient Intelligence and Humanized Computing*, 1-11.

[13] Qureshi, K. N., Din, S., Jeon, G., & Piccialli, F. (2020). Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges With Future Aspects. *IEEE Transactions on Intelligent Transportation Systems*.

[14] Rani, S. S., Alzubi, J. A., Lakshmanaprabu, S. K., Gupta, D., & Manikandan, R. (2019). Optimal users based secure data transmission on the internet of healthcare things (IoHT) with lightweight block ciphers. *Multimedia Tools and Applications*, 1-20.

[15] Reddy, D. S. (2019). Probabilistic Model for Optimal Cell Selection for Seamless Handover in LTE/LTE-A Networks. *Indian Journal of Public Health Research & Development*, *10*(5), 992-1000.

[16] Robinson, Y. H., & Julie, E. G. (2019). MTPKM: Multipart trust based public key management technique to reduce security vulnerability in mobile ad-hoc networks. *Wireless Personal Communications*, *109*(2), 739-760.

[17] Stamou, A., Dimitriou, N., Kontovasilis, K., & Papavassiliou, S. (2019). Autonomic handover management for heterogeneous networks in a future internet context: A survey. *IEEE Communications Surveys & Tutorials*, *21*(4), 3274-3297.

[18] Tang, J., Wen, H., Zeng, K., Liao, R. F., Pan, F., & Hu, L. (2019). Light-weight physical layer enhanced security schemes for 5G wireless networks. *IEEE Network*, *33*(5), 126-133.

[19] Tayyab, M., Gelabert, X., & Jäntti, R. (2019). A survey on handover management: From LTE to NR. *IEEE Access*, *7*, 118907-118930.

[20] Vien, Q. T., Le, T. A., Yang, X. S., & Duong, T. Q. (2019). Enhancing security of MME handover via fractional programming and Firefly algorithm. *IEEE Transactions on Communications*, *67*(9), 6206-6220.

[21] Wang, Y., Zhang, P., Zhou, Y., Yuan, J., Liu, F., & Li, G. (2010). Handover management in enhanced MIH framework for heterogeneous wireless networks environment. *Wireless Personal Communications*, *52*(3), 615-636.

ISSN: 2582-4104
Submitted: 06.12.2020
Accepted: 29.12.2020
Published: 05.01.2021