Bio-inspired Authentication of MTC in Long Term Evolution Networks

Amandeep Singh Dr. Charanjit Singh

Department of Electronics and Communication Engineering, Punjabi University, Patiala, India
Department of Electronics and Communication Engineering, Punjabi University, Patiala, India

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 16 April 2021

Abstract: The evolution of communication technology results in an open, flexible, and heterogeneous wireless network that is more susceptible to malicious attacks. Under such scenarios, massive M2M communication will lead to increase latency and requires more bandwidth. To deal with the network attacks to offer improved QoS is the major challenge in real-time MTC applications. In the paper, a nature-inspired and highly secure mechanism is proposed to authenticate the available respondents based on the fitness function of Artificial Bee Colony (ABC) algorithm and the relationship factor, which is computed in the light of the past performance of the respondents using CRITIC method. The source shares the encrypted data with the respondents that can be decrypted at the terminal based on the key sharing mechanism. The performance of the proposed work mechanism is computed in terms of bandwidth consumption and computation complexity. Simulation analysis against 1000 MTC devices with variable number of intermediate hopes demonstrates that the proposed work exhibits 13% to 14% lesser bandwidth consumption along with 17% lesser computation complexity involved in offering authenticated communication in the LTE network.

Keywords: MTC, ABC, CRITIC Method, Authentication, Bandwidth, and Computation Complexity

Introduction

The communication can be done using any available means, namely, wired, wireless, or their combination. Since the last decades, cellular technology has been extensively evolving from 1G to 5G, as illustrated by the timeline shown in Figure 1 (Taufique et al., 2017). The salient features exhibited by each technical generation had attracted numerous applications from time to time. However, the first generation technology was mainly concerned and was exclusively aimed to serve society. As the trend moved further, the idea to keep minimal base stations came into existence. However, this doesn't fit the growing challenges and leads to crowded networks at the beginning of the '20s. The attraction towards multimedia applications involving audio, video streaming, online gaming involved high data usage. This lead to the advent of the third generation partnership project (3GPP) under the name of LTE technology followed by LTE-A which had been the significant events in the rejuvenation of communication technology (Wang and Yeh, 2011). The LTE technology offered high-speed data transmission with low latency and flexible bandwidth but with variable security. Irrespective of the physical layers and the bandwidth adapted for the communication, fifth-generation is expected to enhance communication systems' capacity.

It has been predicted that the connection density will reach 1 million km2 with around 100 billion connections (Cao, 2018). While comparing the past and the present market trends for mobile communication, it is expected that by 2026, even 6G technology will enter the mobile communication market (David and Berndt, 2018).

The most common feature of the technology-driven world of automation is human to machine communication and vice-versa. The machines here generally refer to the IoT and MTC devices. As the number of connected MTC devices is expected to increase, the security concerns will become challenged due to unauthorized access are also expected to rise.

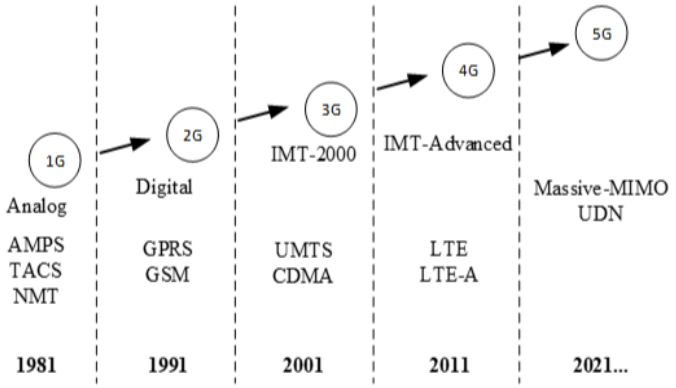

Figure 1: Evolution of Cellular Technology Generations

Security has been an open issue and to secure high-speed LTE network a large number of Authentication and Key Agreement (AKA) schemes such as EPS-AKA (Haddad et al., 2010; Lai et al., 2013; Alezabi et al., 2014) have come to existence. In fact, it is observed that the LTE technology came with some major drawbacks:

- Firstly, network security such as replay, DoS, impersonation and eavesdropping attack, etc.
- Secondly, existence of imperfect forward secrecy and backward secrecy.

Therefore, to offer high level security, twin authentication is required, i.e., at user level and at device level. The emerging ultra-dense network needs to precisely study in terms of self–organizing operations to design automated techniques. Here, ML algorithms' integration to authenticate the network proves to be very promising to handle the adjoining uncertainties and action responses of the dynamic architecture (Sharma and Wang, 2019).

In M2M communication, the MTC devices send requests to access to the network. This process results in computational cost and signaling overhead and may results in congestion at some of the critical nodes. Therefore, in more recent works, grouping methods have been implemented to optimize the M2M communication and the access mechanism. A comprehensive study of grouping based authentication protocols is discussed under literature section.

Contribution of the paper

The paper includes a nature-inspired scheme for group-based authentication architecture for M2M communication. The major contribution of the paper are as follows:

- ABC is implemented as an optimization approach to approve the respondent reply for authentication purpose based on relationship factor and QoS parameters.
- The critic method is used to normalize the QoS parameters for network evaluation.
- The relationship factor is used to provide due weightage to the past record of the respondent.

Organization of the paper

The paper is divided into 5 sections. Section 1 introduces the evolution of cellular communication and needs to integrate authentication with automation. Section 2 discusses the protocols developed for the authentication based on the idea of grouping MTC devices. The architecture of the proposed swarm intelligence inspired group-based authentication protocols is discussed in section 3 with simulation parameters and performance analysis summarized in section 4. The paper is concluded in section 5 with list of bibliographic notes cited in the paper.

Table 1: List of Abbreviation

Abbreviation	*Description*
ABC	*Artificial Bee Colony*
AKA	*Authentication and Key Agreement*
CRITIC	*Criteria Importance through Inter-criteria Correlation*
DoS	*Denial-of-Service*
E-ABC	*Enhanced-ABC*
ECDH	*Elliptic Curve based Diffie-Hellman*
EPS-AKA	*Evolved Packet System Authentication and Key Agreement*
G- AKA	*Group Authentication and Key Agreement*
GBAAM-AKA	*Group-based access authentication for MTC AKA*
GBS-AKA	*Group-Based Secure Authentication and Key Agreement*
GLARM	*Group-based Lightweight Authentication scheme for Resource- constrained M2M communications*
GR-AKA	*Group Based Authentication and Key Agreement*
GTK	*Group Temporary Key*
HSS	*Home Subscriber Server*
IMSI	*International Mobile Subscriber Identity*
IoT	*Internet-of-Things*
LSTM	*Long Short Term Memory*
LTE	*Long Term Evolution*
LTE-A	*LTE-Advanced*
M2M	*Machine-To-Machine*
MD	*Maximum Distance*
MiTM	*Man in the Middle*
ML	*Machine Learning*

MME	*Mobile Management Entity*
MTC	*Machine-Type-Communication*
QoS	*Quality of Service*
RSA	*Rivest, Shamir and Adleman*
SE-AKA	*Security Enhanced Authentication and Key Agreement*
SI	*Swarm Intelligence*
SPEKE	*Simple Password Exponential Key Exchange*
SRGH-AKA	*Secure and Robust Group-Based Handover AKA*
WiMAX-A	*Worldwide Interoperability for Microwave Access.*

Literature Survey

The section convers the existing work that addressed the network security and authentication in LTE and LTE-A networks. The idea of grouping MTC devices was initially implemented to address the issues of network congestion. The protocols designated a group leader that was responsible for data transmission in order to reduce network overhead (Jung et al., 2010). This idea is further extended for authenticating MTC devices to secure data transmission and communication among large sized networks. In the same year, Haddad had proposed EPS-AKA to secure LTE network. The scheme was majorly aimed to resolve transmission issues of IMSI to protect the network against malicious attacks. The public key encryption was used to secure transmitted messages using RSA However, it inhabited the major LTE drawbacks namely privacy preservation and forward and backward secrecy and the biggest challenge was observed for group based authentication (Haddad et al., 2010)). Later, its enhanced version of EPS-AKA was proposed to offer mutual online entity authentication between groups of mobile stations. The performance analysis of showed that it offered better authentication but with a challenged execution time (Chen et al., 2012). To fit the group authentication scenarios in LTE networks, SE-AKA protocol was proposed by Lai. The protocol took advantage of asymmetric key crypto currency for privacy protection and ECDH for forward and backward secrecy with relatively a reliable performance in terms of computation cost and communication overhead (Lai et al., 2013). The local group of MTC devices were authenticated using EG-AKA in non-3GPP networks. However, the implemented protocol remains vulnerable to network attacks such as MiTM and DoS with high computational cost (Jiang et al., 2013). It was observed that the security issues arising due to malicious attacks results in significant end-to-end delay during communication. To address this, SPEKE inspired protocol was designed that was faster that the certificate based schemes (Alezabi et al., 2014).

The selection between symmetric and asymmetric cryptography was the key concern with the passing time while implementing key-based encryption algorithms. The merits and limitations of implementing symmetric and asymmetric key cryptography were studied by Chandra et al. It was established that symmetric key encryption is based on a single key for both encryption and decryption during transmission may become insecure. Therefore, asymmetric key cryptography was found to be better to offer secure data transmission (Chandra et al., 2014). Cao proposed two group-based authentication schemes in 2015 in which first MD group leaves the current eNB to move to the terminal eNB and then the terminal eNB authenticate the rest of MD in the MTC. The scheme significantly reduced the communication cost and signalling overhead. However, due to asymmetric cryptography's involvement, the overall computational cost gets significantly increased (Cao et al., 2015). An asynchronous secrete key distribution was used by Li et al. in the proposed GR-AKA protocol. The Diffie-Hellman key exchange method was integrated to the group authentication scheme to offer distributed authentication in LTE-A network. The comparative analysis against the existing authentication protocols, the proposed GR-AKA could authenticate MTC devices and dynamically update access control policy (Li et al., 2015). In NOVEL-AKA protocol, the HSS was used to compute GTK to authenticate MTC devices. The rest of the MTC devices present in the local group were then validated by MME while HSS remains the crucial factor for authentication. However, it cannot fully secure the data communication against some network attacks (Lai et al., 2015).

In contrast to this, Choi had presented a G-AKA protocol that could successfully authenticate MTC devices against network attacks with small signaling overhead. The protocol proposed by Li et al. exhibited challenged privacy rendering the group of MTC devices more venerable to identity theft (Choi et al., 2015). Another group signature-based protocol was proposed by Cao in which aggregated the signatures were sent to group leader that are in turn forwarded to MME for verification and crosschecking against respective MTC devices. It was a highly authenticated protocol but suffered significant computational overhead (Cao et al., 2015). The number of unnecessary signals observed during data transmission were reduced using GBS-AKA scheme. The scheme proved to reduce the communication delay and protect network against attacks significantly. GBS-AKA scheme outperformed the existing group authentication protocols in terms of bandwidth consumption (Yao et al., 2016). Another improvement in the group based authentication protocols was proposed by Fu et al. with integration of elliptic curve cryptography. The proposed protocol was named as PRIVACY-AKA in which HSS authenticates MME and validates the MTC devices present in the group. The implementation of asymmetric cryptography

results in high security but the network overhead gets significantly increased (Fu et al., 2016). GLARM-AKA was another group-based authentication protocol proposed by Lai that comprises of combination of GLARM-1 and GLARM-2. This light-weight technique could address the network issues and exhibited lower network overhead to meet resource constraint MTC devices' requirements. On the other hand, security aspects get challenged due to fact that group of MTC devices could easily join and leave as renders the open paths for nodes and unfortunately for DoS attack too (Lai et al., 2016).

Parne had analysed that group authentication protocols mainly relies on the pre-shared symmetric or asymmetric keys. During data transmission, the keys may get victim to malicious attacks that compromise the whole system's security. Therefore, SEGB-AKA protocols was introduced in which NSP governed the key generation and authentication. The choice of group leader totally depends on the power consumption and battery life. However, the computation cost of this protocol also remained high (Parne et al., 2018). Later in 2018, Cao et al. addressed the LTE technology's security issues based on authentication protocols in MTC devices. The performance was analysed in the present of attacks and it was observed that the work outperformed the existing mechanisms and protocols in terms of bandwidth consumption and signaling overhead while securing against malicious attacks with variation in the number of respondents. (Cao et al., 2018). The authentication issues related to mass MTC devices were addressed using SRGH-AKA protocol on LTE-A network. The protocol implemented a group key updated mechanism bestowed with forward and backward privacy. The accuracy of formal and informal inspection to offer secure transmission among MTC devices was computed using AVIDPA tool (Gupta et al., 2019). Alezabi proposed authentication and re-authentication scheme for LTE-A and WiMAX-A. The protocol majorly focused on minimizing the signaling cost between UEs and the authentication server and results in reduced handover cost and delay of 22% and 44% at low energy consumption. (Alezabi et al., 2020). It has been observed that the idea of group based communication to offer security proved to be very successful with some of the adjoining imperfections also listed in Table 2 that let vulnerabilities peep into the network.

Table 2: Literature review of group-based authentication protocols

Year	*Protocols*	*Type of Authentication*	*Cons*	*Left Vulnerability*
2013	*SE-AKA*	*Deployed Asymmetric cryptography*	*High Signaling overhead*	*MiTM, DoS, spoofing*
2013	*EG-AKA*	*Authentication of non- 3GPP network*	*High Computational overload*	*MiTM, Impersonation, Node replication threat, spoofing*
2015	*G-AKA*	*Entity-based Mutual Authentication*	*High Computational Cost*	*MiTM, DoS, Impersonation, Node replication threat, spoofing*
2015	*GBAAM-AKA*	*Signature-based Authentication*	*High Computational Cost*	*Node replication threat, spoofing*
2016	*Novel AKA*	*Entity-based Mutual Authentication*	*DoS infused redirection attacks*	*MiTM, spoofing*
2016	*GLARM-AKA*	*Group-based Lightweight cryptography*	*Weak unlink ability for forward and backward secrecy*	*Impersonation, Node replication threat, spoofing*
2016	*Privacy-AKA*	*Pseudo Identity Via ECC based mutual authentication*	*Weak key forward secrecy*	*Impersonation, Node replication threat*
2016	*GR-AKA*	*Flexible policy using Lagrange*	*High bandwidth consumption*	*Node replication threat*
2016	*GBS-AKA*	*Secure Entity-based Authentication*	*Weak unlink ability for forward and backward secrecy*	*MiTM, Node replication threat, spoofing*
2018	*SEGB-AKA*	*Public key based*	*Weak unlink*	*Impersonation,*

		Authentication	*ability for forward and backward secrecy*	*Node replication threat, spoofing*

In addition to the improvement in the existing group-based authentication protocols, ML techniques' rising popularity for addressing the authentication issues have also been observed. Zhao outlined the salient features of MTC architecture and its role and relationship with the evolving LTE technology and the rising network threats that compromise the security aspects. Further, some of the possible solutions to secure M2M communication in heterogeneous network were also presented. Zhao had employed a fingerprint of hardware to design a cross layer authentication to identify the source of the broadcasted message (Zhao et al., 2017). The continuously evolving communication technology is moving into the era of 5G that requires more innovative approaches to secure network against diverse types of attacks. To address this, virtual network anomaly detection modules were designed by Maimó based on deep learning architecture and LSTM (Maimó et al., 2017). Jyothi and Chaudhari had proposed a swarm intelligence inspired ML technique to construct an attack detection model to secure M2M communication (Jyothi and Chaudhari, 2020). Fu adopted another heuristic mechanism as an adaptive approach for data security over LTE/LTE-A (Fu et al., 2020) and identification of rogue stations (Jin et al., 2019).

Motivation

An uninterrupted and fast internet service is a highly challenging task due to the presence of heterogeneous MTC devices in the network that are required to support multiple applications. Additionally, the incidences of data breaches and the malicious attacks remain the open areas of research requiring designing and deploying secure and authenticated data transmission among MTC devices. The existing group based approaches has inspired the authors to design highly secure communication to overcome the limitations related to bandwidth and computational cost. Here, integration of group based authentication with ML and SI techniques is another solution to resolve existing protocols' limitations.

Methodology

The proposed work is highly motivated with the idea of group based authentication of MTC devices to secure data communication and integrated the ML and SI techniques to resolve the limitations in terms of bandwidth and computation cost. The work considers the broastcast replies from the MTC devices and is proposed as a communication as well as an authentication mechanism. The interpolation architecture using curve fitting is applied in the proposed ML inspired GbAS. The replies are evaluated using ABC as SI approach to authenticate the respondents. The overall architecture is shown in Figure 2.

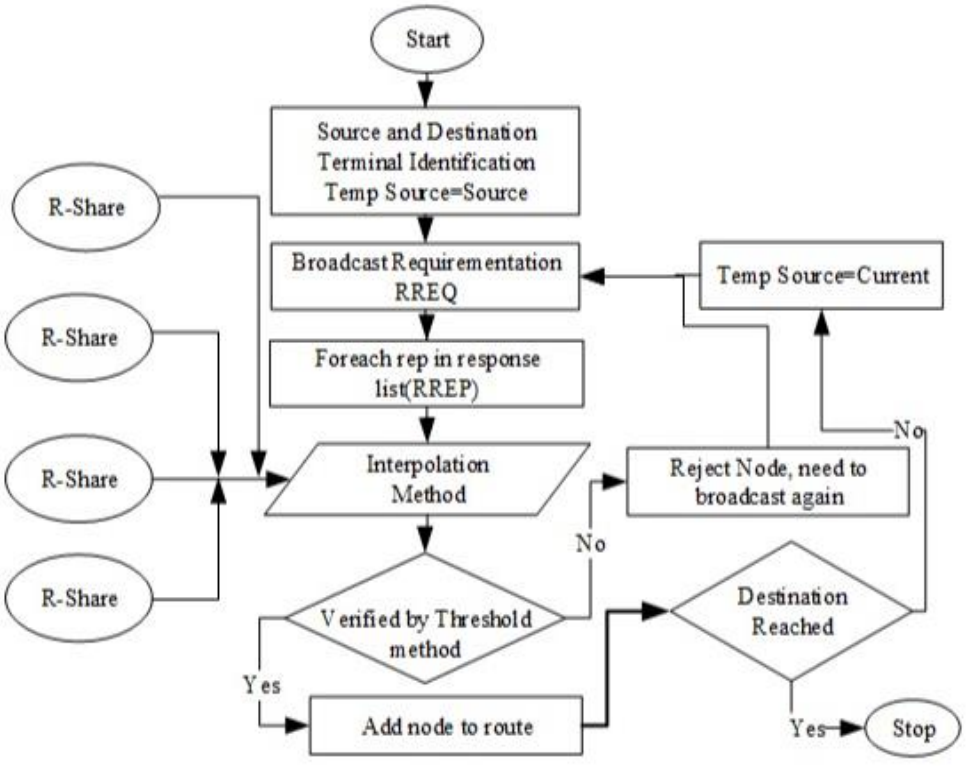

Figure 2: Overall architecture of the proposed work

Network Deployment

The designed network follows 3GPP architecture with number of access points with defined source and terminal as described in Table 3. The location is further subdivided into 9 set of areas with identical configuration as illustrated in Figure 3.

Table 3: Network Architecture

Parameter	*Description*
Network Architecture	*3GPP*
Area	*1000m × 1000m*
Distribution	*Random*
Defined Access Points	*Source and Destination Terminal*

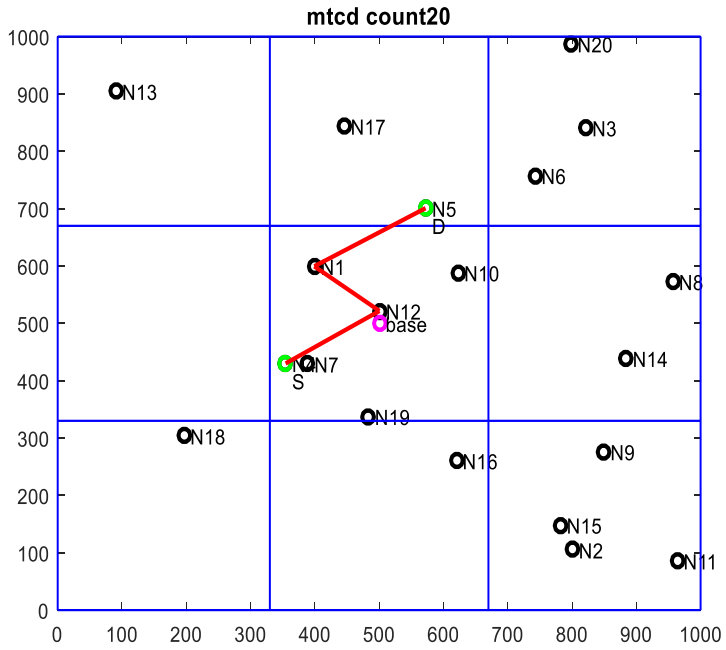

Figure 3: Node deployment and root discovery

Once the source and the destination terminals are defined, the root discovery mechanism is applied to trace the communication path from the source to the destination terminal as illustrated in Figure 2. Here number of possibilities arise. As illustrated in Figure 3 there could be multiple hops present between the two terminals. Similarly, there could also be multiple number of source and the destination that used to share the same set of hops in the earlier path discoveries.

Proposed Architecture

The proposed algorithm is aimed at transferring data through secure MTC devices in the network. The data is divided into regions and now the respondent list is prepared to compensate the deployed MTCs. The idea here is to minimise the security breaches and reduce network overload with one network key for the entire network because otherwise due to generation of mesh of keys will increase the network time and increases more time available for security breaches.

The work relies on a set of two algorithms: SI approach and the interpolation architecture. A number of nature inspired algorithms are available that can be used for analysing group behaviour (Beni, 2020). Out of various SI approaches, an enhanced-ABC is implemented for analysing the group behaviour of MTC devices involved in the network. In the proposed E-ABC, there are two bees involved one each representing the parameters of QoS namely, throughput and delay. The algorithmic structure is shown as pseudo code and the architecture of E-ABC is illustrated in Figure 4.

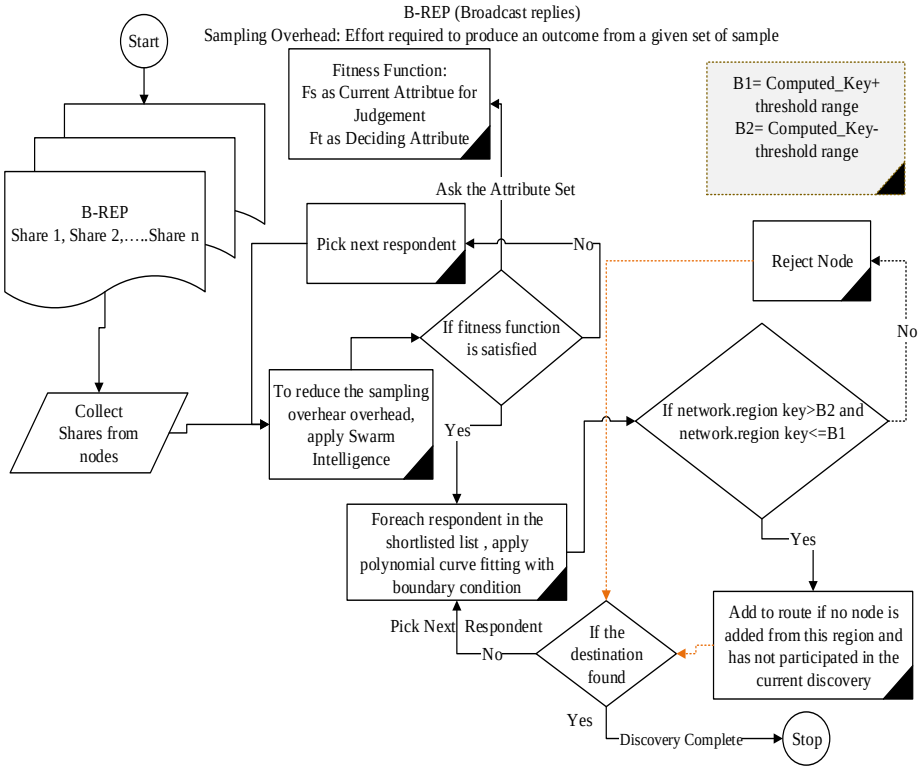

Figure 4: Enhancement in ABC algorithm

Here, E-ABC acts as a selection mechanism and the interpolation algorithm verifies the respondent to be added to the hop to the discovery path or not. In this context, a share verification is applied for the set of nodes or respondents based on twin mechanism used by E-ABC:

- Every respondent has a share based on the network that has been generated in the light of its record of offering secure communication. It is also called the relationship factor. If the respondent had any record of secure transmission, it assigned a relationship factor of 0.1.
- Another scoring is based on QoS parameters, namely, throughput and delay. In fact, these parameters differ in terms of metrics and units, and therefore they are normalized using CRITIC method.

CRITIC method was initially introduced by Diakoulaki et al. in 1995 and evaluated the decision matrix and standard deviation to find the correlation between the two QoS parameters. For each criteria (X_ij) correlation function (R_ij) that translates all the values of criteria i.e. F_j Into interval [0,1] is expressed as;

$$R_{ij} = \frac{x_{ij} - x_j^{minimum}}{x_j^{maximum} - x_j^{minimum}} \quad (1)$$

This transformation is based on the ideal point concept in which the initial matrix is transformed into a matrix having generic elements i.e. R_{ij}.

The fitness function is designed in such a manner that it takes into consideration both types of nodes:

- The nodes that have earlier communication relation with the considered node.
- The nodes with no earlier communication relation with the considered node and assigned a correlation value of 0.

The normalized throughput and delay is used in the fitness function to compute the correlation factor.

$$Correlation_{factor} = Correlation_{value} + \frac{n-Throughput}{n-Delay} \quad (2)$$

The respondent nodes that qualify the fitness function are moved to the respondent list that are cross-verified by the polynomial curve fitting using the pseudo code whose work flow is illustrated in Figure 5.

Algorithm: Pseudo Code for Proposed Algorithm

1. Input: List of Node (N_L)Source (S_r), Destination (T_r), Background Correlation (Bg_{Corr}), Quality of Standard Repository $(QoS_{Rep})Route_{Request}$ $initiated\ from\ Source\_node$
2. $For_{each}\ rep\ in\ RREP$
3. $f = Validate\ Bg_{Corr}\ for\ corelation_{score}\ (C_S)$
4. $f = 1,\ if\ found\ co-relation$
5. $0, Otherwise$
6. $If\ f == 1, corelation_{score}\ (C_S) = .10$
7. $Else, corelation_{score}\ (C_S) = 0$
8. $Js_{Rep} = \frac{N\_Throughput\_Rep}{N\_Delay\_Rep}$
9. $Applicable\ List\ (App_{Lst}) = Initialize\ to\ Empty$
10. $Apply\ fitness\ function\ (Ft_f) of\ ABC$
11. $If\ is\ satisfied\ Ft_f, add\ note\ to\ possible_{solution}\ for\ process\ of\ route\ discovery$
12. $Apply\ Poly_{Fit}\ Curve_{Fitting}$
13. $Input\ to\ Poly_{Fit} - shares\ of\ possible_{solution}$
14. $Network\_key = Determine\ network\_key\ from\ repository$
15. $Determine\ respons e_{key} using\ shares\ for\ at\ least\ interpolation\ (3rd\ order)$
16. $In\ 3rd\ order\ interpolation\ at\ least\ three\ members\ are\ used\ for\ computation$
17. $If\ 2\ out\ of\ 3\ are\ rejected, then\ 3rd\ node\ will\ be\ rejected\ automatically\ rejected$
18. $First\ boundary\ value\ (B_{val_1}) = Network\_key + boundary\ \%$
19. $Second\ boundry\ value (B_{val_2}) = Network_{key} - boundary\ \%$
20. $The\ boundary\ value\ vary\ in\ the\ range\ of$ 10% to 30% in presented work
21. $If\ Evaluated\ Key\ (Ev_{Key}) > B_{val_2}\ \&\&\ Ev_{Key} < B_{val_2}$
22. $Accept_{node}$
23. $Else$
24. $Reject_{node}$
25. End_{if}
26. $Compute\ highest\ judgement\ value\ (jud_{Val}) and\ add\ node\ to\ the\ list\ of\ route$
27. $Update\ list\ of\ route\ for\ future\ communication\ reference$
28. Obtained Output: Discovered Route (Dis_{Route})

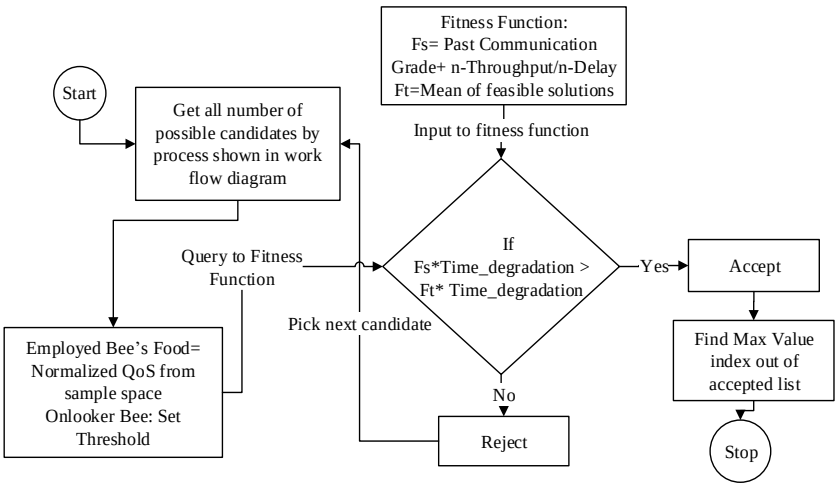

Figure 5: Evaluation of respondent replies

Results and Discussion

The proposed algorithm discussed in the last section utilizes ML architecture to offer group based authentication of data transmission from source to destination terminal to offer high end security. The key sharing mechanism has been applied to protect the data and select the best hop to continue the transmission process. The transmitted data utilized a specified bandwidth and if results in high bandwidth consumption and computation complexity the overall cost of data transmission becomes very high. Therefore, these two are the majorly evaluated in this section. The performance evaluation of the proposed work is analysed against the existing group based authentication protocols to justify the proposed work's effectiveness. The network simulations are performed in MATLAB simulator and parametric values against bandwidth and computation complexity are determined against number of MTC devices. The authentication message is calculated for the proposed work using the following equation.

$$BW_{MTC} = \sum_{i=1}^{5} |msg_i| \quad (3)$$

Where bandwidth for each MTC device is computed as BW_{MTC} and the message is represented as msg.

The bandwidth is further analysed by varying the number of hops in the deployed network. When the number of hops are restricted to be below 5, the computed bandwidth is variation with the increase in the number of MTC devices is illustrated in Figure 6. It is observed that when data transmission is performed using less number of hops the bandwidth consumption of the proposed ML approach is less than the existing group based protocols. The average bandwidth consumption of the GBS-AKA, S-AKA, G-AKA, SE-AKA, GR-AKA, GLARM-1, and GLARM-2 is 0.0997Mbps, 0.7266Mbps, 0.5183Mbps, 0.7447Mbps, 0.3735Mbps, 0.1047Mbps, and 0.1028Mbps, respectively. However, the proposed work exhibits the average bandwidth consumption of 0.0857Mbps which is $\left(0.0997 - 0.0857/_{0.0997}\right) * 100 = 14.05\%$ less than the protocol demonstrating the least bandwidth consumption.

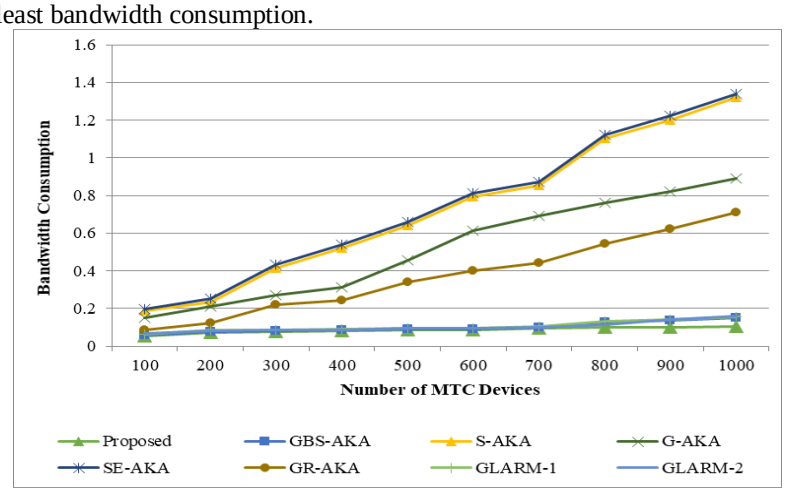

Figure 6: Bandwidth consumption when number of intermediate hops < 5

Now, the number of hops is increased, and all the protocols' bandwidth consumption is further analysed. Figure 7 illustrates the bandwidth consumption change when the number of intermediate hops is between 5 and 8. It is observed that when the number of intermediate hops increases, the bandwidth consumption of all the protocols also increases. At this stage, the average bandwidth consumption of GBS-AKA, S-AKA, G-AKA, SE-AKA, GR-AKA, GLARM-1, and GLARM-2 is 0.2228Mbps, 0.7352Mbps, 0.550Mbps, 0.7679Mbps, 0.4056Mbps, 0.2229Mbps, and 0.2264Mbps, respectively. This demonstrates that when the number of intermediate hops are more than 5 but still less than 8, the average bandwidth consumption of the proposed work is $\left(0.2228 - 0.1919/_{0.2228}\right) * 100 = 13.86\%$ less than the best performing protocol.

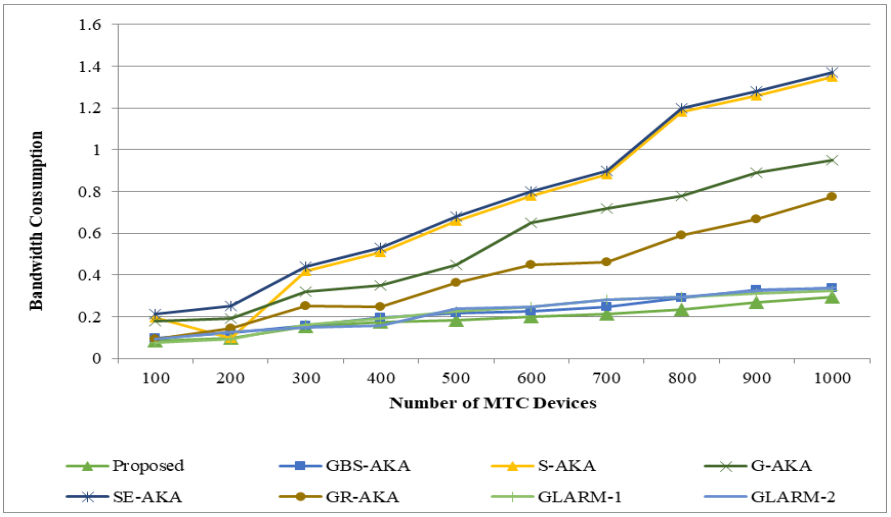

Figure 7: Bandwidth Consumption when intermediate hops > 5 but < 8

The effect of a further increase in the number of intermediate hops on bandwidth consumption is illustrated in Figure 8 where a number of hops lie between 8 and 10. A similar trend is observed in this case too as the bandwidth consumption increases again when the number of intermediate hops increases. This is reflected in terms of increased average bandwidth consumption of 0.2505Mbps, 0.8614 Mbps, 0.6558 Mbps, 0.8571 Mbps, 0.4547 Mbps, 0.2577 Mbps, 0.2633 Mbps and 0.2163 Mbps for GBS-AKA, S-AKA, G-AKA, SE-AKA, GR-AKA, GLARM-1, GLARM-2, and proposed work, respectively.

The average bandwidth consumption of the proposed work is found to be $\left(0.2505 - 0.2163 / 0.2505\right) * 100 = 13.68\%$ less than the least bandwidth-consuming protocol.

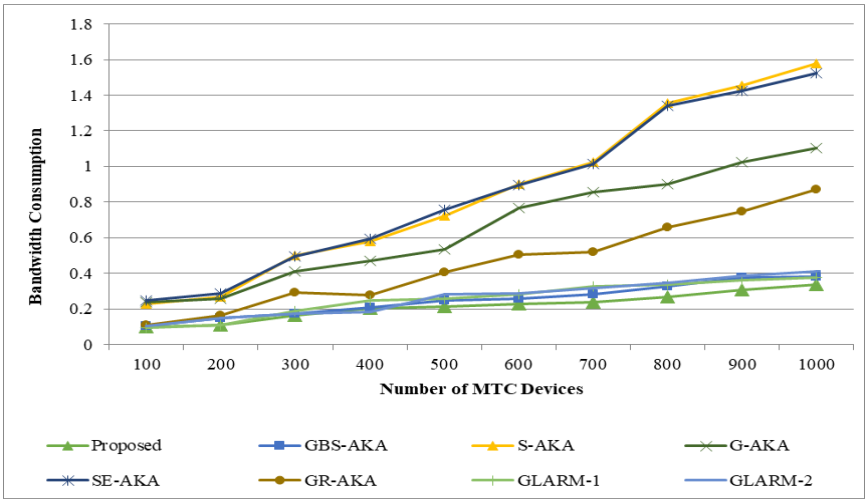

Figure 8: Bandwidth Consumption when intermediate hops > 8 but < 10

A comparative analysis of these average bandwidth consumptions of these protocols in comparison to the existing ML inspired group authentication work is illustrated in Figure 9. The three set of observations inferred from the figure are as follows:

- It is generalized that an increase in the number of intermediate hops increases the average bandwidth consumption of all the techniques.
- Secondly, overall analysis shows that the proposed ML integrated architecture exhibits the least bandwidth consumption among all the existing techniques under study.
- Thirdly, based on the bandwidth consumption, the proposed work's performance is very near to GBS-AKA and GLARM protocols.

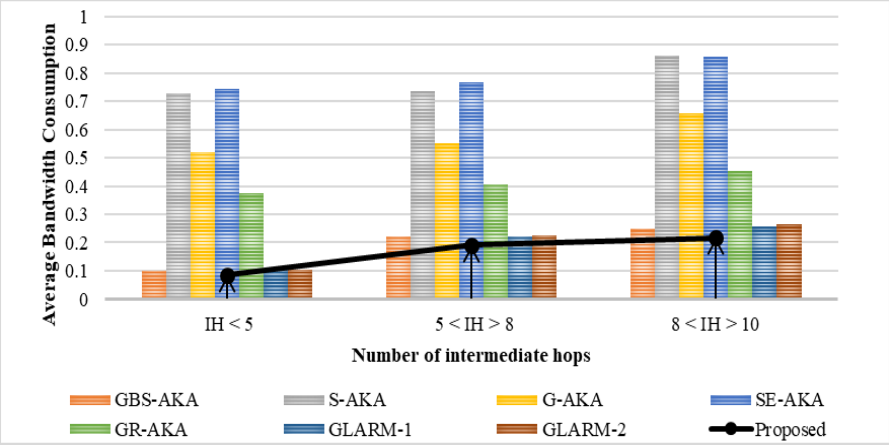

Figure 9: Average Bandwidth Consumption under three scenarios

The GBS-AKA had employed entity based authentication, while GLARM utilized group based lightweight cryptography and the proposed work group based authentication inspired from GLARM protocol has been utilized. Therefore, next the performance of the proposed ML inspired group based authentication work is compared for the computation complexity against the GLARM protocol proposed by Lai et al.

The Computation Complexity ($C_{complex}$) reflects the total time lapsed or consumed to transfer data from source to the destination terminal to complete the process of data transmission. It can be further represented by the following equation.

$$C_{complex} = \sum_{i=1}^{p} Mes_{time} \quad (4)$$

It covers the time required to authenticate the nodes or the MTC devices and the intermediate elements to offer secure communication. The type of authentication majorly governs the variation in the computation complexity. The computation complexity of the proposed work is compared with the Lai et al.'s work (GLARM) and Lopes et al.'s work in figure 10.

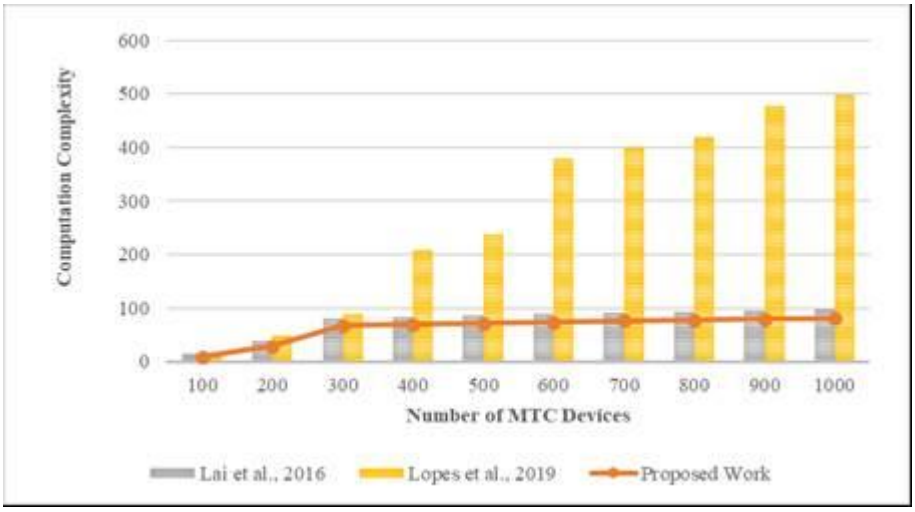

Figure 10: Computation Complexity Analysis

The existing literature employed several variations in the authentication mechanisms in terms of ciphering architecture that majorly governed the computation complexity of their respective works. E-ABC is utilized as the SI approach in the proposed work that considerably minimized the time required to authenticate the MTC devices. Therefore, the computation complexity of the proposed work gets significantly reduced. The average computation complexity of 63.7ms, 77.4ms, and 277.8ms has been observed for the proposed work, Lai et al. work, and Lopes et al. work. This means that the proposed work exhibits $\left(77.4 - 63.7/77.4\right) * 100 = 17.70\%$ lesser computation complexity to authenticate and complete the data

transmission process based on a group-based authentication mechanism observed against variation in the number of MTC devices used for performance analysis.

Conclusion

The paper introduces a bioinspired group-based authentication scheme to optimize the authentication process integrating interpolation architecture and CRITIC methods. The E-ABC is utilized as a selection mechanism to determine the authentication of the respondent machines that are further cross-validated by CRITIC method. The proposed work's performance is first analysed in terms of bandwidth consumption while varying the number of intermediate hops required for data transmission. It was observed that with an increase in the number of intermediate hops the bandwidth consumption also increases; however, the bandwidth consumption of the proposed work remained minimum among all the studies. Next, the paper's performance determinant factor is computation complexity that reflects the time consumed to offer a secure communication process. In this case, the proposed work outperformed the existing protocols due to the integrations of ML and SI techniques that significantly reduced the time consumed during the authentication process. It is observed that when a large number of MTC devices access and communicate through the LTE network, the proposed work could significantly reduce the network overhead and cost. Overall, it is inferred that the employed mechanism reduced the higher bandwidth consumption and the computation complexity required for mutual authentication between-group head and MTC members. The paper also inspires the research community to integrate more advanced ML techniques to address the challenges of communication in LTE network.

REFERENCES

1. Alezabi, Kamal Ali, Fazirulhisyam Hashim, Shaiful J. Hashim, Borhanuddin M. Ali, and Abbas Jamalipour. "Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks." EURASIP Journal on Wireless Communications and Networking 2020 (2020): 1-34.
2. Alezabi, Kamal Ali, Fazirulhisyam Hashim, Shaiful Jahari Hashim, and Borhanuddin M. Ali. "An efficient authentication and key agreement protocol for 4G (LTE) networks." In 2014 IEEE Region 10 Symposium, pp. 502-507. IEEE, 2014.
3. Beni, Gerardo. "Swarm intelligence." Complex Social and Behavioral Systems: Game Theory and Agent-Based Models (2020): 791-818.
4. Cao, Jin, Hui Li, and Maode Ma. "GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks." In 2015 IEEE International Conference on Communications (ICC), pp. 3020-3025. IEEE, 2015.
5. Cao, Jin, Maode Ma, and Hui Li. "GBAAM: group-based access authentication for MTC in LTE networks." Security and communication networks 8, no. 17 (2015): 3282-3299.
6. Cao, Jin, Maode Ma, Hui Li, Yulong Fu, and Xuefeng Liu. "EGHR: Efficient group-based handover authentication protocols for mMTC in 5G wireless networks." Journal of Network and Computer Applications 102 (2018): 1-16.
7. Chandra, Sourabh, Smita Paira, Sk Safikul Alam, and Goutam Sanyal. "A comparative survey of symmetric and asymmetric key cryptography." In 2014 international conference on electronics, communication and computational engineering (ICECCE), pp. 83-93. IEEE, 2014.
8. Chen, Yu-Wen, Jui-Tang Wang, Kuang-Hui Chi, and Chien-Chao Tseng. "Group-based authentication and key agreement." Wireless Personal Communications 62, no. 4 (2012): 965-979.
9. Choi, Daesung, Hyoung-Kee Choi, and Se-Young Lee. "A group-based security protocol for machine-type communications in LTE-advanced." Wireless networks 21, no. 2 (2015): 405-419.
10. David, Klaus, and Hendrik Berndt. "6G vision and requirements: Is there any need for beyond 5G?." IEEE Vehicular Technology Magazine 13, no. 3 (2018): 72-80.
11. Fu, Anmin, Jianye Song, Shuai Li, Gongxuan Zhang, and Yuqing Zhang. "A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks." Security and Communication Networks 9, no. 13 (2016): 2002-2014.
12. Fu, Yulong, Hanlu Chen, Qinghua Zheng, Zheng Yan, Raimo Kantola, Xuyang Jing, Jin Cao, and Hui Li. "An Adaptive Security Data Collection and Composition Recognition method for security measurement over LTE/LTE-A networks." Journal of Network and Computer Applications 155 (2020): 102549.
13. Gupta, Shubham, Balu L. Parne, and Narendra S. Chaudhari. "SRGH: A secure and robust group-based handover AKA protocol for MTC in LTE-A networks." International Journal of Communication Systems 32, no. 8 (2019): e3934.
14. Haddad, Zaher, Sanaa Taha, and Imane Sarwat. "SEPS-AKA: A secure evolved packet system authentication and key agreement scheme for LTE-A networks." Computer Science & Information Technology (CS & IT) 1, no. 5 (2010): 57-70.

15. Jiang, Rong, Chengzhe Lai, Jun Luo, Xiaoping Wang, and Hong Wang. "EAP-based group authentication and key agreement protocol for machine-type communications." International Journal of Distributed Sensor Networks 9, no. 11 (2013): 304601.
16. Jin, Jian, ChangLiang Lian, and Ming Xu. "Rogue Base Station Detection Using a Machine Learning Approach." In 2019 28th Wireless and Optical Communications Conference (WOCC), pp. 1-5. IEEE, 2019.
17. Jung, Kwang-Ryul, Aesoon Park, and Sungwon Lee. "Machine-type-communication (MTC) device grouping algorithm for congestion avoidance of MTC oriented LTE network." In International Conference on Security-Enriched Urban Computing and Smart Grid, pp. 167-178. Springer, Berlin, Heidelberg, 2010.
18. Jyothi, K. Krishna, and Shilpa Chaudhari. "Optimized neural network model for attack detection in LTE network." Computers & Electrical Engineering 88 (2020): 106879.
19. Lai, Chengzhe, Hui Li, Rongxing Lu, and Xuemin Sherman Shen. "SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks." Computer Networks 57, no. 17 (2013): 3492-3510.
20. Lai, Chengzhe, Hui Li, Xiaoqing Li, and Jin Cao. "A novel group access authentication and key agreement protocol for machine-type communication." Transactions on emerging telecommunications technologies 26, no. 3 (2015): 414-431.
21. Lai, Chengzhe, Rongxing Lu, Dong Zheng, Hui Li, and Xuemin Sherman Shen. "GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications." Computer Networks 99 (2016): 66-81.
22. Li, Jinguo, Mi Wen, and Tao Zhang. "Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks." IEEE Internet of Things Journal 3, no. 3 (2015): 408-417.
23. Lopes, Ana Paula G., Lucas O. Hilgert, Paulo RL Gondim, and Jaime Lloret. "Secret sharing-based authentication and key agreement protocol for machine-type communications." International Journal of Distributed Sensor Networks 15, no. 4 (2019): 1550147719841003.
24. Maimó, Lorenzo Fernández, Félix J. García Clemente, Manuel Gil Pérez, and Gregorio Martínez Pérez. "On the performance of a deep learning-based anomaly detection system for 5G networks." In 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), pp. 1-8. IEEE, 2017.
25. Parne, Balu L., Shubham Gupta, and Narendra S. Chaudhari. "Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network." IEEE Access 6 (2018): 3668-3684.
26. Sharma, Shree Krishna, and Xianbin Wang. "Toward massive machine type communications in ultra-dense cellular IoT networks: Current issues and machine learning-assisted solutions." IEEE Communications Surveys & Tutorials 22, no. 1 (2019): 426-471.
27. Taufique, Azar, Mona Jaber, Ali Imran, Zaher Dawy, and Elias Yacoub. "Planning wireless cellular networks of future: Outlook, challenges and opportunities." IEEE Access 5 (2017): 4821-4845.
28. Wang, Li-Chun, and Chu-Jung Yeh. "3-cell network MIMO architectures with sectorization and fractional frequency reuse." IEEE journal on selected areas in Communications 29, no. 6 (2011): 1185-1199.
29. Yao, Jiming, Tao Wang, Mingkai Chen, Lei Wang, and Gejuan Chen. "GBS-AKA: Group-based secure authentication and key agreement for M2M in 4G network." In 2016 International Conference on Cloud Computing Research and Innovations (ICCCRI), pp. 42-48. IEEE, 2016.
30. Zhao, Caidan, Lianfen Huang, Yifeng Zhao, and Xiaojiang Du. "Secure machine-type communications toward LTE heterogeneous networks." IEEE Wireless Communications 24, no. 1 (2017): 82-87.