Multi-layer Authentication and Key Agreement Protocol for Secured Data Transmission in Cloud-RAN

Awaneesh Kumar Yadav*, Byomakesh Mahapatra†, Shailesh Kumar ‡, Ashok Kumar Turuk§
Dept. of Computer Science and Engineering
National Institute of Technology, Rourkela, Odisha, India
*Email: [*217cs2312, †514cs6020, ‡ 518cs1014, § akturuk] @nitrkl.ac.in*

***Abstract*—The rapid increase in global data traffic increases the load and insecurity at the present radio access network architecture. This limitation of the present network leads to redesign the base station architecture. The centralized/cloud radio access network (C-RAN) technology consider being an alternative solution for the next-generation base station. This architecture performs a centralized processing and controlling activity at central location instead of the distributed processing as in traditional BS. As the C-RAN has centralized and collaborative processing, it has the capability to overcome many security challenges and proved itself to be a secured, energy and cost efficient architecture for the next generation cellular network. Different types of threats and attacks are possible at different layers of C-RAN. In this paper, we have proposed a multi-layer authentication and key agreement protocol (ML-AKA) for securing all layers of C-RAN to establish an end to end connection between the user entity (UE). This proposed protocol is to authenticate and validated by AVISPA and the simulation result shows that the proposed ML-AKA protocol reduces the chance of attacks to a greater extent.**

***Keywords*—Base station, C-RAN, DoS, DDoS, ML-AKA, Network Security.**

I. Introduction

As the wireless and cellular network is moving towards 5^{th} generation the utilization of the wireless terminal data traffic is growing rapidly. According to a study conducted by Cisco, the per-user data traffic has increased from 30 MB to 2000 MB from 2012 to 2017 per month and it is expected to reach 10 GB till the end of 2020. Again the global wireless devices which are connected to the base station (BS) and wireless access point (AP) increase from 7 billion to 10.3 billion in 2012 to 2017, with an annual compound growth rate of 8.3% [1]. To mitigate this rapid increase in wireless and cellular devices and to avoid the limitation of conventional Radio Access Networks (RAN) a centralized interface management is required for the next-generation cellular network. There are various limitations such as high-cost incurred, limited bandwidth, and huge power consumption limits the scalability and flexibility of the present base station. The cloud-RAN emphasizes on this limitation and redesigned the RAN architecture with a centralized control and management system. This new architecture not only reduces the involve cost incurred such as capital expenditure (CAPEX) or operational expenditure but also help to design an energy efficient network. In comparison to the traditional BS, the C-RAN architecture consists of a distributed radio unit also known as remote radio head (RRH) and a centralized processing unit known as a baseband unit (C-BBU) [2]. Both the RRH and BBU are connected through a high bandwidth fronthaul link which may be a wired or wireless type.

In C-RAN, the RRHs collects the incoming signals from the wireless devices and transfer to the BBUs through the wireless fronthaul link. The received baseband signal processing and controlling activity is carried out at the Baseband Units (BBUs) or BBU-pool. The C-RAN can also be categorized into three layers such as :

- *Device layer :* It consists of different cellular and wireless devices which are connected to the RRH through a wireless link.
- *Link layer :* The link layer consists of the Fronthaul and Backhaul link which connect the RRH to the BBU and BBU to the core network respectively.
- *Physical base band layer :* This layer consists of the C-BBU and the core network which performs all the controlling and processing activity. This C-BBU can also be grown over a conventional data center by using the virtualization and cloud computing technology [3].

As these three-layers exchange the data and information for providing services to the end user, the security and privacy issues are the key factor in implementing C-RAN technology. Except the data security and privacy issues the C-RAN has also the different problem like access control, robustness, integrity, authentication, trustworthiness, non-repudiation etc are the key concept to established a secure end to end communication. The important man-made system attacks which mainly affect the device layer of the C-RAN are distributed denial of services (DDoS), impersonation and eavesdropping attacks. The wireless link layer is mainly affected by jamming or DoS attack. As the BBU or physical processing layer uses virtualized and cloud computing technology which leads to many attacks like DoS attack, SQL injection, physical access, spear phishing etc. are possible. As the DoS attack is a primary attack which effects all the layer of the C-RAN [4]. In this paper, we have proposed an ML-AKA protocol to reduce the effect of DoS and DDoS attacks in C-RAN. The rest of the

978-1-5386-8235-7/18/$31.00 ©2018 IEEE

paper is as follow; Section II. described the prior related work carried out by earlier researcher focusing on C-RAN and its security issues. Section III. described the security requirement for C-RAN for an end to end communication. Section IV. focused on different security issue and vulnerability in C-RAN and discuss different possible security issues for C-RAN in more detail. In Section V the proposed protocol is given followed by its mathematical and flow diagrams. The simulation result and protocol validation are given in Section VI. Finally, in Section VII, a concluding remark is given for this paper..

II. Literature Survey and Prior Related work

The physical implementation of cloud based BS or C-RAN raised many security challenges for the implementation of next generation network [5]. Different organization and research group are working to avoid this attacks. In [6], authors have suggested a layered architecture for C-RAN, which divides whole architecture into three planes i.e. physical plane, control plane and service plane. In [7], authors have discussed different threats and security issues at different layers of the 5G network which also discussed the C-RAN security as an open research issue for future network implementation. In [8], author has discussed about key agreement and authentication for secure communication. Authors in [9], focused on the different security issues and corresponding solution for the virtualized and cloud platform at the BBU layer. The paper also discussed the cloud security alliance which is a key factor to provide platform as a service (PaaS) to different internet services and telecom service providers. In [10], the author has discussed the effect of a DDoS attack and defense mechanism. In [11], the author's discuss different 4G cellular network threats and given an attacker model for the cellular network. In [12], the authors analyzed two types of improper behavior of DoS attack and selfish misbehavior. The adversary model present in the paper, discuss how malicious node disturb the network traffic by sending heavy network traffic. In [13], the authors discussed the common jamming threat and proposed the different solution for this jamming attack. Although all these papers have focused on the many security challenges for cellular and wireless network, no paper has given a concrete security model and its corresponding solution for C-RAN architecture.

III. Security Parameters for C-RAN Architecture

For a secure C-RAN system different security parameters that must be follow to ensure the safety of the whole network architecture are as follows

A. Authentication

Authentication is the most important security requirement for the C-RAN system. It uses the different techniques to authenticate the authorized user for a secured communication and link control. In C-RAN authentication, needs at each layer to verify who performs what. By using proper authentication technique it is easy to detect the malicious user, which helps to overcome attacks like DoS attack and Reply attacks.

B. Integrity and Confidentiality

Integrity ensures that the system, the component, and transmitted information are secured and unchanged. Confidentiality ensures the secrecy of users information. In the C-RAN system, the essential element of confidentiality is data generated by user devices at the device layer, access data at the link layer and the processing data at the physical BBU layer. Integrity ensures the data associated with the different layer of C-RAN are legal un-altered and non-corrupted.

C. Privacy

In the C-RAN system, privacy exists among operators and end users. Privacy of end users are defined as personal information privacy, data privacy, and identity privacy. Service providers uses different privacy preservation techniques at the different layer of the C-RAN based on some service level agreement (SLA). The user or device link with any network must be ensured with this SLA for a secured communication.

D. Trustworthiness

C-RAN has a lot of advantages over traditional RAN such as highly scalable and flexible to accommodate a different kind of cellular user in term of operator and services specific. There should be cooperation among mobile operators when going for an IaaS scenario. A secure trust management mechanism is established for collaboration among operators through which we can get an effective solution for virtualized threats.

E. Non-Repudiation

There should be liability between the user and mobile service providers. To ensure an end to end communication, all the layers should be integrated toward a global solution and authentication. Any layer should not deny the authorized user request without the acknowledgment of other layers.

F. Access control to resource

This is one of the most important security requirement in the C-RAN system . Resources and services should be accessible only for authorized users anywhere and anytime. it gives the effective solution for impersonation attack.

IV. Security Threats and Vulnerability in C-RAN

As different layers of C-RAN affected by different man made security threats, which limits the functionality and performances of this architecture. The main security threats for the different layer of the C-RAN architecture are as follows:

A. Security threats and vulnerabilities in Device layer

Device Layer Consists of all the physical devices such as cellular and wireless devices and its corresponding nodes. For access control and to establish a D2D or D2X communication, security and privacy are the prime concerns for this layer. The two most common attack for this layers is DDoS and Eavesdropping.

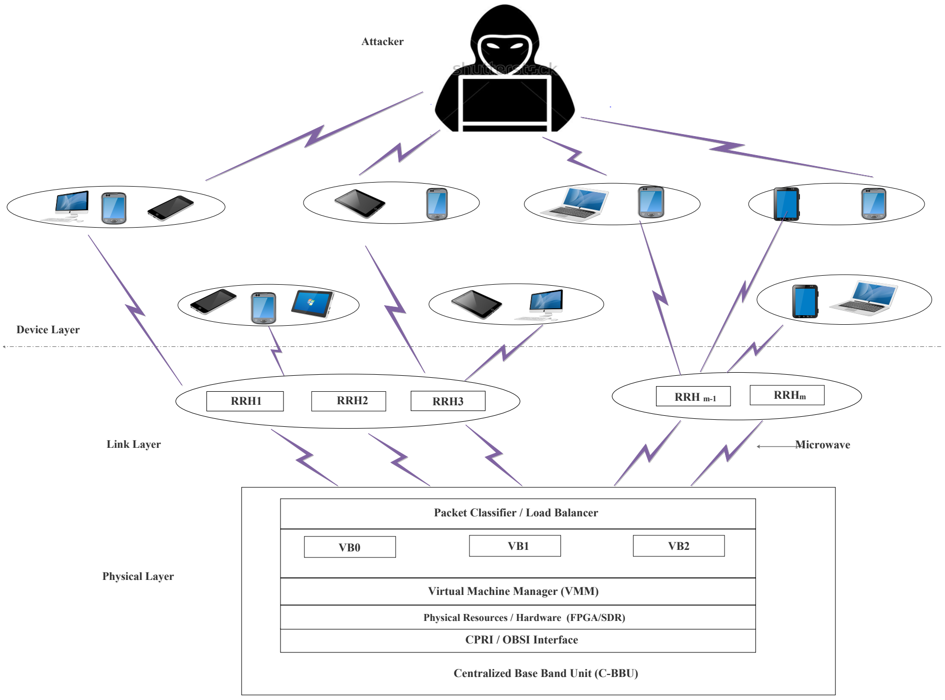

Attacker
Device Layer
RRH1
RRH2
RRH3
RRH m-1
RRHm
Link Layer
Microwave
Packet Classifier / Load Balancer
VB0
VB1
VB2
Physical Layer
Virtual Machine Manager (VMM)
Physical Resources / Hardware (FPGA/SDR)
CPRI / OBSI Interface
Centralized Base Band Unit (C-BBU)

Fig. 1. Attacker Model for C-RAN

1) Distributed denial of services attack (DDoS): In the device layer, the Attacker can compromised some user devices which will act as botnet (A group of the compromised device or infected device by an attacker). After establishing the botnet, the attacker has full remote control over the devices. Through which it can send the unauthorized traffic to disturb the normal traffic of the network. In the DDoS attack, attacker attacks on the large set of devices in a network, due to this compromised devices occupies the major part of the network bandwidth, which hampers the normal network services for the authorized users.

2) Eavesdropping: Eavesdropping is a possible attack through which the device layer can get affected. It is an attack in which an attacker can intercept the private conversation over a network to get sensitive information. It is also defined as a violation of confidentiality. The eavesdropping can be possible in two way i.e

- Attacker can violate this by directly access the private conversation between sender and receiver over a digital media.
- Another way attacker access the valuable information by using interception or sniffing technique.

B. Security threats and vulnerabilities in Link layer

The link layer of C-RAN consists of RRH, wireless fronthaul, and an optical backhaul link. The User Entity (UE) link with the RRH through a secured wireless channel to transfer information and data. The link layer is mainly affected by DoS attack or jamming attack. DoS attack is possible in the RRH unit because it receives the signals from a large number of connected devices, processed it and sends it to the upper layer. If any attacker attacks the corresponding connected devices and sends a huge number of unauthorized request to the RRH. As the RRH has limited bandwidth to handle the requests, the larger number of requests create a jamming problem at the RRH and its corresponding front haul link.

C. Security threats and vulnerabilities in physical base band layer

The C-BBU in the physical layer is used as a platform for the different type of services and operators. Data security and privacy are the prime factors for providing services to the end user. As it uses the cloud computing and virtualization techniques for C-RAN implementation, many types of attacks are possible at BBU and core network. The different possible attacks in this layer are as follows:

1) Denial of services (DoS) attack : DoS attack can occur in BBU of the virtualization environment, an end user can use the same machine with numerous operating system in which virtual machine shares resources like CPU, storage (memory or disk) and network. The main target of the adversary is to weak the resource from the physical host to disturb the services of the other virtual machine in BBU.

2) Privacy threat : The privacy of devices can be easily violated. In C-RAN Architecture, idle spectrum resources are allocated to the devices based on the devices geographic locations. Due to this process, device's private key may be stolen by unauthorized parties. Thus, devices privacy should be considered.

V. The Proposed ML-AKA Protocol for C-RAN Layered Architecture

In the C-RAN layered architecture, several attacks are possible at the different layers. To avoid these attacks in this paper we have proposed a secure and efficient Multi-layer Authentication and Key Agreement (ML-AKA) protocol for the C-RAN application. In this proposed protocol three layer authentication required for secure end to end communication The different layer of authentication are given known as :

- Device layer authentication (DLA).
- Link layer authentication (LLA).
- Physical base band layer (PBBU) Authentication

Each layer of C-RAN requires authentication and key registration for each connected devices. This process is carried out in three different phase like; User Entity (UE) registration, link setup, session key establishment phase as shown in Fig. 2.

A. User Entity (UE) registration

The UE are associated and registered with a particular RRH during the UE registration phase. To establish an end to end connection the registration process is carried out in different steps :

1) End user devices (UE_i where i = 1,2) send the registration request to RRH_j for accessing the local area service. The identities of end user devices (UE_1, UE_2) are used for the registration process of UE to their respective RRH.
2) The RRH_j will accept the request coming from UE_i and sends it to the BBU for authentication with their own identity ($RRHID_j$) for the verification process.
3) In the next phase the UE register to the BBU along with the RRH id $RRHID_j$. BBU will accept the RRH request and verify the legitimacy of the RRH_j. If authentication request send by the authorized end user device (UE_i) and Remote Radio Head ($RRHID_j$) is valid, then BBU will simply accept it and produce authentication information that contain Kj_{asme} registration key with the help of key distribution function (KDF). If the authentication information is not valid then BBU rejects the UE request.

$$Kj_{asme} = KDF(K_j, RRHID_j, rand_j) \qquad (1)$$

Where: K_j Secret key between device and BBU and $rand_j$ is the random number chosen by BBU.

4) After receiving the authentication information (kj_{asme}) form BBU, RRH_j and UE_i will mutually authenticate each other. For the mutual authentication and key agreement process UE_i and RRH_j derived the function key Kj_{U2U} with help of Kj_{asme}.

$$Kj_{U2U} = KDF(Kj_{same}, f_{id}, rand_j) \qquad (2)$$

where f_{id} is U2U function identity and $rand_j$ is random chosen by RRH_j . The U2U session key generated by the U2U fun key Kj_{U2U}

B. Link setup and authentication phase

After UE registration process, the link is established between the UE, RRH and BBU. If another UE associated with the same RRH and BBU, they communicate each other by sharing a random secret Key M_j. If random secret key M_j validate with random secret key of other device then link setup phase will takes place.

C. Session key establishment phase

After the link setup and authentication phase, session establishment is carried out between the UE through the RRH and BBU. The complete process is carried out in following sequences steps.

1) One of the end user device UE_2 request for the session key creation by sending session request to the RRH_j. For the session request UE_2 send it own identity along with identities of the receiver RRH and UE (UE_2, UE_1, $RRHID_1$ and r_1) to the $RRHID_2$. Then this request is forwarded to the BBU_2.
2) After accepting the session request, BBU_2 verify the legitimacy of the corresponding device. BBU_2 will accept session request only for legitimate device. It will send UE_1, UE_2, r_1 and SID_1 to the BBU_1 .
Where SID_1 Session identity of end user device and UE_1 and r_1 random number
3) In the next step the BBU_1 will verify the legitimacy of key agreement request send by BBU_2 and accept the services. BBU_1 send another random number r_2 with (UE_1, UE_2) to BBU_2.
4) BBU_2 and BBU_1 creates a pre-shared key by exchanging the random nonce value which is calculated by XOR function. The pre-shared key K_{ps} sends a session confirmation to the corresponding devices UE_1, through the RRH_1.
5) End user device UE_1 and UE_2 will create the session key S_1 and S_2 by choosing random number a and b. The message authentication code M_1 and M_2 are computed for S_1 and S_2 with the help of hashed mac and common secret shared key before exchanging the session keys.

$$M_1 = HM_{K_{cm}}(S_1, t_1) \qquad (3)$$

$$M_2 = HM_{K_{cm}}(S_2, t_2) \qquad (4)$$

t_1 and t_2 are time-stamps, where K_{cm} = K_{RRH} XOR K_{ps}.

6) End user devices UE_1 and UE_2 will check the correctness of the time stamp after receiving the S_1 and S_2, which is computed by the hashed mac and their common pre-shared key K_{ps}. If both side verification result matched then they create the U2U session key KS_{U2U} = $(S_1)^b$ = $(S_2)^a$ and protect communications using the common session key KS_{U2U} subsequently.

$$K^j_{asme} = KDF(K_j, BBU_{id}, rand_j) \qquad (5)$$

$$K^j_{U2U} = KDF(K^j_{asme}, f_{id}, rand_j) \qquad (6)$$

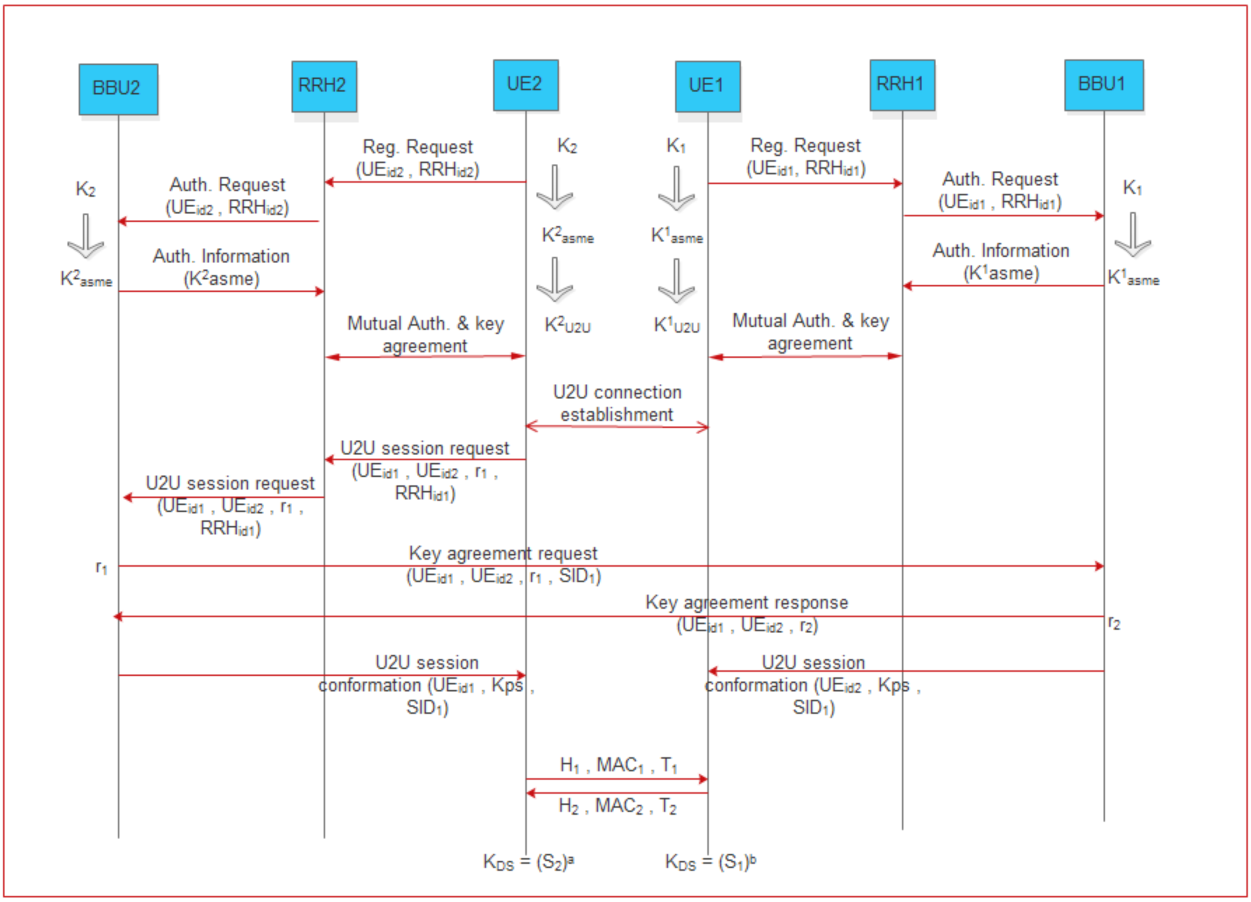

BBU2
RRH2
UE2
UE1
RRH1
BBU1
Reg. Request (UEid2 , RRHid2)
K2
K1
Reg. Request (UEid1, RRHid1)
K2
Auth. Request (UEid2 , RRHid2)
K2asme
K1asme
Auth. Request (UEid1 , RRHid1)
K1
K2asme
Auth. Information (K2asme)
Auth. Information (K1asme)
K1asme
K2U2U
K1U2U
Mutual Auth. & key agreement
Mutual Auth. & key agreement
U2U connection establishment
U2U session request (UEid1 , UEid2 , r1 , RRHid1)
U2U session request (UEid1 , UEid2 , r1 , RRHid1)
r1
Key agreement request (UEid1 , UEid2 , r1 , SID1)
Key agreement response (UEid1 , UEid2 , r2)
r2
U2U session conformation (UEid1 , Kps , SID1)
U2U session conformation (UEid2 , Kps , SID1)
H1 , MAC1 , T1
H2 , MAC2 , T2
KDS = (S2)a
KDS = (S1)b

Fig. 2. ML-AKA protocol for the C-RAN network.

$$K_{ps} = r_1 XOR r_2 \tag{7}$$

$$K_{cm} = R_{RRH} XOR K_{ps} \tag{8}$$

$$S_1 = (g)^a, S_2 = (g)^b \tag{9}$$

$$M_1 = HMAC_{K_{cm}}(S_1, t_1) \tag{10}$$

$$M_2 = HMAC_{K_{cm}}(S_2, t_2) \tag{11}$$

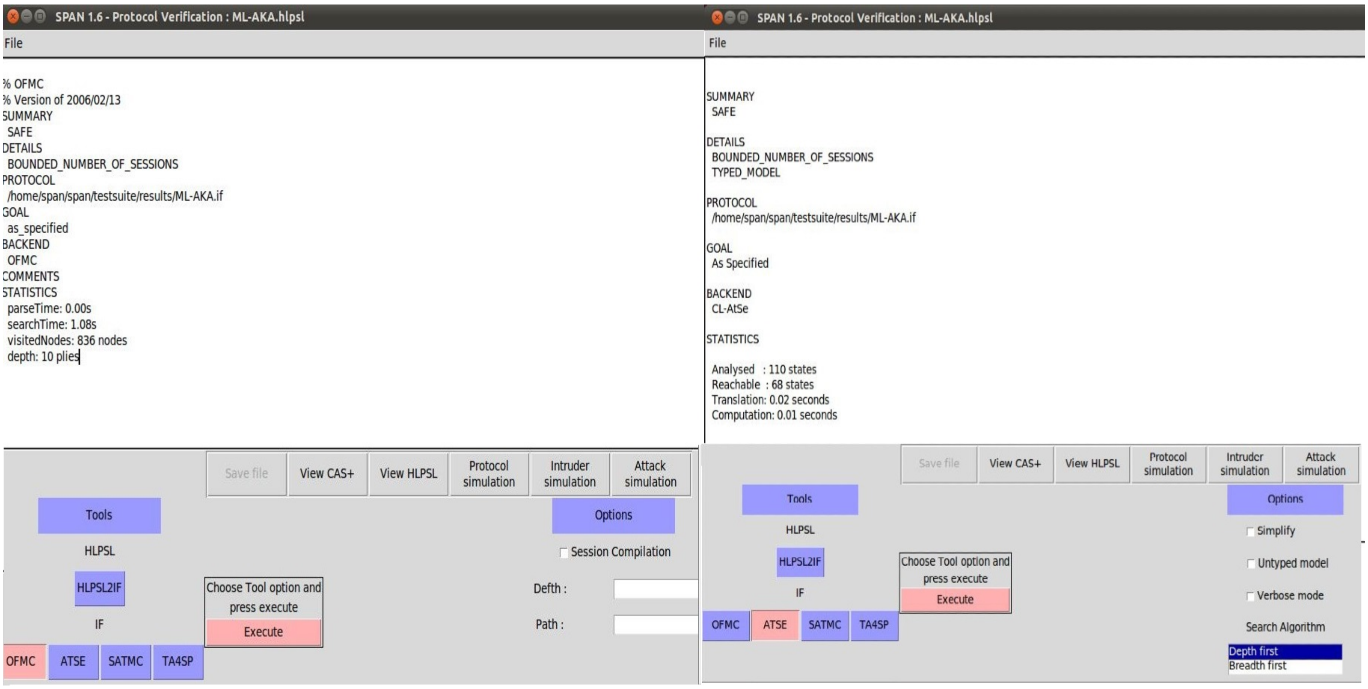
$$K_{DS} = (S_1)^b = (S_2)^a \tag{12}$$

VI. Simulation and Results

We have simulated the proposed protocol using Automated Validation of Internet Security Protocols and Applications (AVISPA v 1.1) on a Linux OS environment on a system with ACPI X86 based with Intel- i7 process with 8GB RAM [14]. The proposed protocol is simulated for evaluation of a secured data transfers through the different layer of C-RAN. The protocol mainly tested for evaluation of DoS and DDoS attack at the different layer of the C-RAN. This protocol was tested by two modes of the AVISPA tool i.e. On-The-Fly Mode checker (OFMC) and Constraint-Logic-based Attack Searcher (CL-AtSe). In the OFMC backend model, proposed protocol is validated through falsification and bounded verification by traversing through intermediate format (IF) specification in a demand-driven way. It traverses all the 836 nodes arranged in a depth of 10 piles in 0.00s parse time and a search time of 1.08s to verify the whole protocol. In the CL-atSe backend model, it verifies the protocol through heuristics and redundancy elimination technique. By using the heuristic technique it analyzed 110 nodes in which it visits the 68 nodes by taking 0.02s translation time and 0.01 computational time

TABLE I
Symbols and Abbreviations

Symbols and Abbreviations	
Symbols	Definition
BBU	Base Band Unit
UE_j/UE_j	User j and its identity
$RRH_j/RRHID_j$	Remote Radio Head j and its identity
K_j	the shared secret key
KDF	Cryptographic function (Key Derivation Function)
K_{D2D}	Function key
RS_{D2D}	D2D session key
S_i	session key hint of devices
M_i	Message Authentication Code
H_i	Hashed function
rand	Random number
K_{ps}	Pre-shared key
K_{asme}	MME Intermediate key
M	Message authentication code



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/ML-AKA.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 1.08s
  visitedNodes: 836 nodes
  depth: 10 plies
```

□ Session Compilation

Defth :

Path :

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/ML-AKA.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 110 states
  Reachable  : 68 states
  Translation: 0.02 seconds
  Computation: 0.01 seconds
```

□ Simplify

□ Untyped model

□ Verbose mode

Depth first

Breadth first

Fig. 3. Simulation result in OFMC back end and CL-atSe back end of AVISPA tool.

to test the protocol. The test parameter such as parse time (Tp) and search time (Ts) is evaluated by increasing the number of test nodes in different back-end models. The final result is shown in Fig.3 also shows that the proposed protocol is safe from different possible attacks and is suitable for the end to end UE connection establishment in a C-RAN environment.

VII. Conclusion

C-RAN architecture considers being a new collaborative, cost-effective secured network for the next generation base station architecture. As the C-RAN design over a cloud computing and radio access network platform, security from the different threats and attacks are the prime concern to establish an end to end communication. The literature shows that the DoS and DDoS attacks are possible at all the layer of the C-RAN architecture. To secure this layer we have proposed a multilayer security protocol to reduce different security attacks and threats at all the three layers of the C-RAN. The simulation result given in Section VI shows that the proposed ML-AKA is efficiently secured the layered devices from possible attacks in C-RAN.

References

[1] Cisco, Visual Networking Index. ”Global Mobile Data Traffic Forecast Update, *White Paper*,” pp. 2015-2020, 2015.

[2] Y.Lin, L.Shao, Z.Zhu, Q.Wang, and R.K Sabhikhi ” Wireless network cloud: Architecture and system requirements,” *IBM Journal of Research and Development*, vol. 54, no.1, pp. 1-12, 2010.

[3] B. Mahapatra, R. Kumar, S. Kumar and A. K. Turuk, ”A real time packet classification and allocation approach for C-RAN implementation in 5G network,”*International Conference on Recent Advances in Information Technology (RAIT)*, Dhanbad, pp. 1-6 , 2018.

[4] K Sonar, H Upadhyay, ” A survey: DDoS attack on Internet of Things.” *International Journal of Engineering Research and Development*, vol.10, pp. 58-63, Nov. 2014.

[5] B. Mahapatra, R. Kumar, S. Kumar and A. K. Turuk, ”A Heterogeneous Load Balancing Approach in Centralized BBU-Pool of C-RAN Architecture,” *International Conference for Convergence in Technology (I2CT)*, pp. 1-5, 2018.

[6] J. Wu, Z. Zhang, Y. Hong and Y. Wen, ”Cloud radio access network (C-RAN): a primer,” *IEEE Network*, vol. 29, no. 1, pp. 35-41, 2015.

[7] F. Tian, P. Zhang and Z. Yan, ”A Survey on C-RAN Security,” *IEEE Access*, vol. 5, pp. 1372-1386, 2017.

[8] Wang M, Yan Z, Niemi V. ”UAKA-D2D: Universal authentication and key agreement protocol in D2D communications.” *Mobile Networks and Applications*, vol. 1, no. 22(3), pp. 510-525, 2017.

[9] Z. Xiao and Y. Xiao, ”Security and privacy in cloud computing,” *Mobile Networks and Applications*, vol. 15, no. 2, pp. 843-859, 2012.

[10] C. Douligeris and A. Mitrokotsa, ” DDoS attacks and defense mechanisms: a classification, ” *IEEE International Symposium on Signal Processing and Information Technology*, pp. 190-193, 2003.

[11] Y. Park and T. Park, ”A Survey of Security Threats on 4G Networks,” *IEEE Globecom Workshops*, pp. 1-6, 2007.

[12] K Bian, J M Park ” MAC-layer misbehavior in multi-hop cognitive radio networks,” *Conference on Science, Technology, and Entrepreneurship*, pp. 228-248, Aug. 2006.

[13] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos and G. Pantziou, ”A survey on jamming attacks and countermeasures in WSNs,” *IEEE Communications Surveys Tutorials*, vol. 11, no. 4, pp. 42-56, 2003.

[14] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J.Cullar, P. H. Drielsma, P. C. Ham, O. Kouchnarenko, M. Mantovani, and S. Mdersheim, ” The AVISPA tool for the automated validation of internet security protocols and applications,” *International conference on computer aided verification*, pp. 281-285, 2005.