A Secure Key Management and Authentication Protocol for Virtualized-BBU in C-RAN Architecture

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

***Abstract*—The centralization and virtualization of baseband unit (BBU) in cloud radio access network (C-RAN) make the BS platform more scalable and flexible. The C-RAN is a next-generation collaborative RAN architecture develop using cloud computing and virtualization technology. C-RAN provide different radio services over a single platform. In comparison to the traditional BS, the architect of C-RAN has two distinct parts, i.e., a centralized Control Unit (CU) and a distributed unit (DU) known as Remote Radio Head (RRH). The RRH handles the end-user whereas the BBU unit performs the signal processing and controlling activity. The virtualized BBU consist of a set of virtual box (VB) managed by a virtual baseband manger (VBM) or hypervisor. As all the VB growth over a single virtualized BS platform, there is a chance of violation security principle such as data integrity, confidentiality and availability at the BBU. In this paper, we have proposed an authentication protocol to secure and independent operation of VB in a BBU-pool. The proposed protocol use Steiner Triple System (STS) and combinatorial design methods for crucial pre-shared distribution. The proposed protocol simulated with Automated Validation of Internet Security Protocols and Applications (AVISPA) tool. The resiliency of V-BBU is analyzed with the help of STS and simulated with the python programming. The simulation result shows that the resiliency of the system is directly proportional to the number of compromised VB, and the use of proposed key-distribution technique improved the resiliency factor even if the increase in the number of compromised VB.**

***Keywords*—C-RAN, Combinatorial design, Network Security, Resiliency, VB, V-BBU**

I. Introduction

The increase in global cellular and wireless traffic needs to expand the network resource like bandwidth, processing power, and hardware capacity. This increase in traffic leads to the use of some alternative technique at the base band unit. The network operators and cellular service providers cooperatively move toward to develop a new base station architecture (BS) which overcome the limitations of the present BS architecture. The centralized or cloud radio access network is a next-generation BS architecture which use the cloud computing and virtualization technique to provide radio access service [1]. In C-RAN, centralization of the baseband unit reduces overall incurred cost like capital expenditure (CAPEX) and operational expenditure (OPEX). On the other hand, the virtualization increases network the scalability and adaptability of the network [2].

A. Architecture of C-RAN:

The C-RAN architecture can be configured into the three layers :

- *Distributed RF Unit (DU):* The RF layer of C-RAN consists of a radio unit known as remote radio head (RRH), and an antenna unit. The antenna unit is wirelessly connected to the user entity (UE). The RRH unit consists of a transceiver which links to the UE through Uplink/Downlink RF signal in the form of radio channels. The receive radio signal reconverts into optical signal and transfer to BBU-pool [3].
- *Centralized processing unit (CU):* The CU perform all the controlling and signal processing activities on a single platform known as the baseband unit. As the centralized-BBU growth over the cloud platform, it consists of a number of virtual boxes (VB). Each VB is handled a different set of RRH as shown in Fig.1. The BBU also consist of a Host OS along with a virtual baseband manager (VBM) which controlled all the VB.
- *Fronthaul and Backhaul connection:* The Fronthaul is the connection between the DU and CU, which is either an optical cable or wireless connection. The backhaul is the connection between CU and the core network. The backhaul is a large bandwidth optical connection include router and switch to interconnect core network to CU.

In C-RAN, virtualization is used to increase the performance of the baseband unit by creating the VB with the help of a guest operating system (G-OS) [4]. The VBM present inside the V-BBU control and monitor all the VB with the help of a host operating system (H-OS). As the baseband unit growth over a collaborative platform, VB security and integrity are the prime factors for independent operation of VB over a single platform. Each VB in the V-BBU use a unique identity for independent operation. If this key is compromised and get access by another unauthorized user, then various attacks like denial-of-service (DoS) attack, man-in-the-middle attack. the revert-to-snapshot problem, SQL Injection, etc. are possible at the V-BBU. To secure the V-BBU from these attacks the key distribution and key preservation are an essential factor for next-generation cellular BS. In this paper, we have introduced a key distribution scheme for V-BBU, which helps to increase

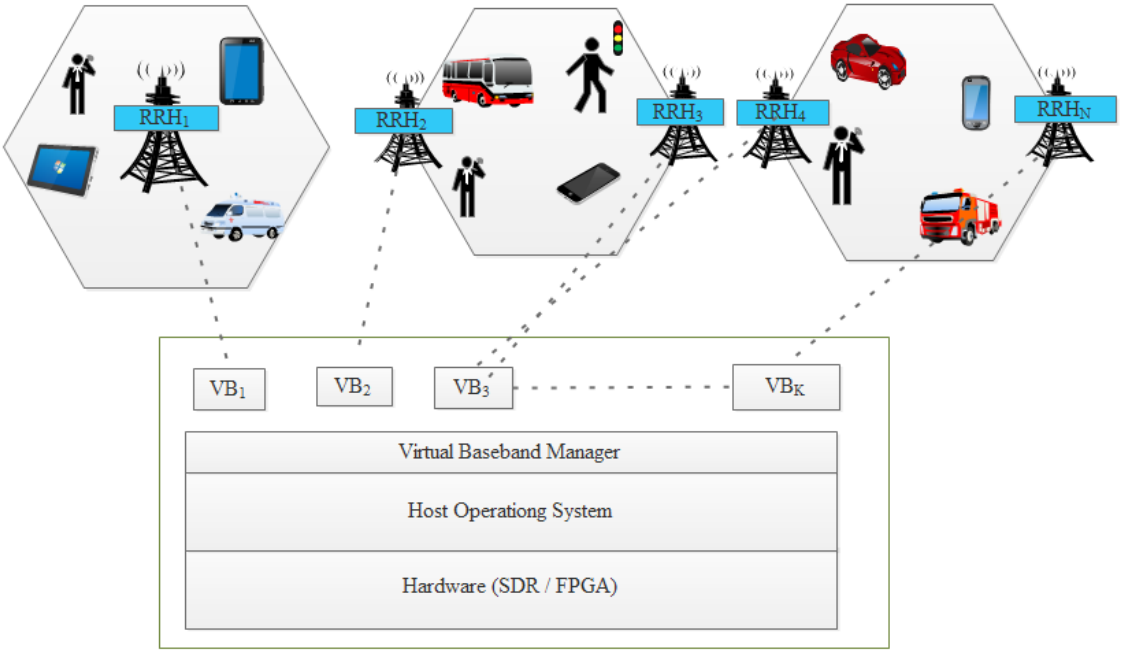

Fig. 1. Architecture of C-RAN with a distributed RRH unit and a virtualized-BBU connected through fronthaul link

the security of the baseband unit by reducing the possible threats and attack. The rest of the paper are arranged as follows. Section II, discussed prior related work on C-RAN and different security model proposed by different authors. Section III, highlights different possible threats attacks in V-BBU of a C-RAN architecture. In Section IV, key distribution and management procedure for C-RAN is discussed. The result and discussion are carried out in Section. V. Finally, the conclusion and future direction of the proposed works is mention in Section VI.

II. Prior Related Work

The baseband unit of C-RAN is a scalable platform which provides radio network as a service (RANaaS) to the multiple cellular operators. All the operators provide services to their customer by creating multiple VB over a single platform. The collaborative radio processing in BBU-pool of C-RAN needs advances security and authentication technique as compared to the traditional BS. In [5], authors focused on different security issue in C-RAN. The paper described the possible attacks and security solution for three different layers i.e. Physical, Media Access Control (MAC), and Radio Resources Control (RRC) layer of C-RAN. Authors in [6], explained about the cloud computing platform and its corresponding security and privacy issue. This paper provides a different solution to maintain cloud confidentiality, integrity, and privacy in a cloud computing platform. In [12], the authors described the virtual machine security in a server of a data-center. The author highlights two important possible attacks i.e attack through the guest-OS and host-OS and proposed the corresponding solution to avoid these attacks.

Key distribution is considered to be an essential factor for independent running of of VBs on a single platform without loss of data integrity and confidentiality. Many research works have done for distribution of pre-shared secret keys in a WSN or cloud environment. Like in [8], the authors proposed a pre-key distribution strategy using Steiner Triple System (STS) in a sensor network. Authors used combinatorial design to distribute the keys among a cluster device in a wireless sensor network. Another work in [9], proposed a key distribution procedure using a combinatorial design for a sensor network. The authors proposed two class of prioritizing connectivity in WSN. The first concept is based on prioritizing connectivity, whereas the second concept is based on resilience properties. Authors in [10], resolve different key distribution issue and proposed different cryptography solution for WSN and cellular networks. All the mention papers are focused on the physical layer security of WSN, cellular network or cloud computing, where has no author focused on the security issues of C-RAN. To fill this void in this work, we proposed an advances key distribution strategy for VB, which helps to perform an independent operation of all active VBs in a BBU.

III. Possible Attacks on V-BBU of C-RAN Architecture

The C-RAN virtual-BBU can be compromised by various attacks due to weak key management. Some of the possible attacks are listed as below:

- **Isolation attack:** Since each VB are independent to each other, they need a unique identity key for their parallel operations in a BBU. If these keys are compromised then it can break the isolation property, as a result other

attacker VB can able to compromised the sources VB and correspondingly changed the properties of that VB.

- **Denial of service attack (DoS):** In the virtualized environment all the physical resources such as CPU, memory, and disk are shared among the VBs. An attacker enters the BBU by creating a fake VB, which acquired most of the bandwidth of the server. This type of attacks is known as a denial of service attack (DoS) in a cloud computing environment. The DoS attack is a universal attack which effects all the layers of C-RAN architecture [13].
- **Migrant attack :** This type of attack generally affects the BBU layer during the process of VB migration. This attack is another form of multi-resource attack, where a third party attacks the source and target BBU during the migration process. The attacker placed a VB in source-BBU and entered into the target-BBU through the migration process and acquired whole bandwidth of target-BBU by compromised its VB [14].
- **Revert to snapshots problem :** Snapshot is a technique that is used to take the snapshot of VB at an instant point and revert the snapshot for the future use if in case of future necessity. If the key is compromised, then the attacker can easily control the whole system in which old details are stored and can access the snapshots [15].
- **Man-In-The-Middle (MITM) Attacks** The MITM attack is a third party attack which intercepts the key exchange process between the sender and receiver in a communication system. The attacker use cryptography public key for accessing the receiver resources. In this scenario, it appears that sender and receiver are communicating with each other, but in reality, the communication is carried out between attacker and receiver. The message receiver does not recognize that the sender is an unknown attacker trying to access or modify the information remotely [16].

IV. Key distribution and management in BBU-pool

The V-BBU consist of a number of VB which are independently run over a host-OS and managed by a hypervisor. To protect the sensitive information during the parallel operations, the BBU use a secret symmetric key to encrypt the identity of each VBs. The communication between the VBs and VBM performs with the help of these key [11, 17]. Various techniques have been used for secure key distribution in WSN and cloud computing environment. In this paper, we present a key distribution strategy using combinatorial design and its underlying steiner triple system (STS). The V-BBU shown in Fig. 2 having N-number of active VB which are currently running, each VB needs a separate identity for independent operation. The KDC assign the key 'K' based on the selection methods. The detail keys selection, distribution and management procedures are as follows:

A. Techniques for keys selection and distribution

- *Combinatorial design:* Combinatorial design theory is use to organising the set of element in a number of subset and each subset represented a symmetric keys as shown in TABLE I.
- *Steiner triple system (STS):* Steiner system is type of combinatorial block design. The STS is based on three parameters S(p, m, l). The subset key for the STS is calculated based on this parameters. Where the parameters p is key pool size, m denotes the key subset block size and l represent repetition rate of keys in key block. All these parameters in the STS should be positive integers and satisfy the following condition $(p > m <= 2)$. A (p, m, l) combinatorial balanced incomplete block design method with control parameters (S, A) have to follow certain properties like :
  - $|S|$ = p,
  - There are m points in each blocks
  - There are several unique points in which every pair of unique points occurred in exactly l block

  Where, S is a universal set of points, and A is group (i.e. multi-set) of non-empty subsets of S called blocks. where:
  $l\ (p-1) = n(m-1)$ and
  $d.m = p.n$.
  In the combinotrial block design based STS method we take m=3, l =1

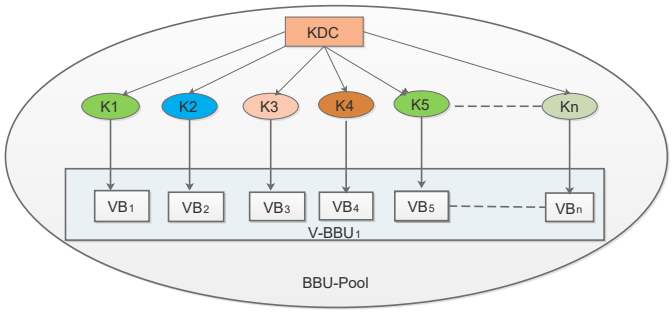

Fig. 2. Selected key assignment to the VBs of a V-BBU

TABLE I
KEY GENERATION FROM THE KEY POOL

Key Management	
Key Pool	A,B,C,D,E,F,G
Generated keys set by combinatorial block design	ABC,ABD,ABE,ABF,ABG,ACD,ACE, ACF,ACG,ADE,ADF,ADG,AEF,AEG, AFG,BCD ,BCE,BCF,BCG,BDE,BDF, BDG,BEF,BEG,BFG,CDE,CDF,CDG ,CEF,CEG,CFG,DEF,DEG,DFG,EFG
Selected key set based on STS	ABC,ADE,AFG,BDF,BEG,CEF,CDG

B. Authentication procedure of VB in V-BBU

Each VB have a unique key use for authentication between VB and VBM. The authentication procedure is carried out in the following steps (Fig. 3):

- A registration request is send by VB to VBM which consist of virtual box ID and detail of resources requirement.

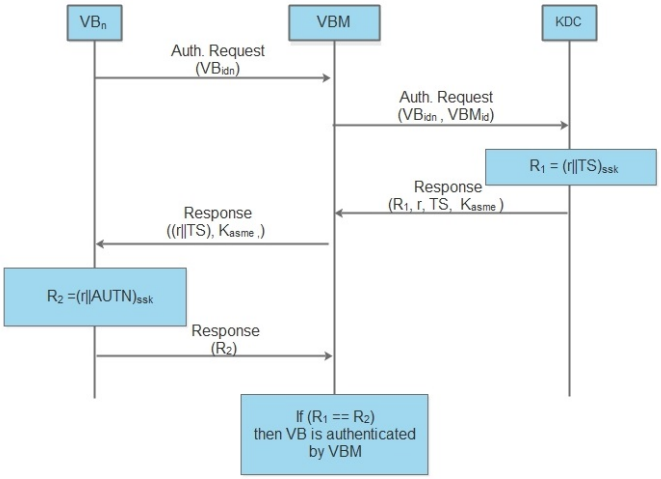

Fig. 3. Authentication procedure of VB in a virtual-BBU

- After accepting the request VBM send it to the KDC to check the authenticity of the machine.
- The KDC accept the request and computes a challenge by using the Pre-Shared secret key that is distributed initially to the VB. It also computes the secret key for verification process K_{asme} by using parameter

$$R_1 = (r||TS)_{(psk)}. \quad (1)$$

$$K_{asme} = KDF(psk, VBM_{id}, TS). \quad (2)$$

- After receiving the challenge VBM will send the parameter to the VB for the verification process and keeps R_1 for further verification.
- After receiving the parameter VB will computes challenge responses with the help of pre-shared secret key for each VB.
- Now VBM check the condition R_1 == R_2. If both the condition is satisfied i.e. a single pre-shared secret key between VB and VBM is same, then request VB is authenticated.

TABLE II
ASSIGNMENT OF SELECTED KEY TO VBS OF A BBU-POOL

Virtual Box	Assigned Keys
VB1	K1 = ABC
VB2	K2 = ADE
VB3	K3 = AFG
VB4	K4 = BDF
VB5	K5 = BEG
VB6	K6 = CEF
VB7	K7 = CDG

C. Resiliency calculation Procedure for V-BBU

In this example, we consider there are seven active VB is currently running in a V-BBU1. The keys for all the active VB is calculated based on the STS which is given TABLE II. We assign one unique key to each VB and measure the efficiency in term of resiliency. Where the resiliency of V-BBU define the ability to provide and maintain the services when there are fault and challenges to normal operation or services. The resiliency of BBU is calculated as:

$$\text{Resiliency of BBU} = \frac{\text{Number of compromised VB}}{\text{Total Number of compromised VB}}$$

V. RESULT AND DISCUSSION

A. Calculation of Resiliency:

The calculation of the resiliency is carried out using Python programming language. Considering the number of VB and its key length as an input parameter as shown in TABLE II, the resiliency of V-BBU is calculated in percentage of compromised as shown in TABLE.III. The increase in the number of compromised VB increased the resiliency of V-BBU as shown in Fig.4. Again the increase in the percentage of compromised VB leads to decrease the processing capability by increasing the overhead associated with the V-BBU operations.

TABLE III
RESILIENCY CALCULATION FOR V-BBU

Resiliency Parameters	10%	20%	30%	40%	50%
P=7, m=3, l=1	0.478	0.496	0.812	0.864	0.874
p=9, m=3, l=1	0.493	0.532	0.814	0.976	0.988
p=13, m=3, l=1	0.512	0.692	0.879	0.988	0.997

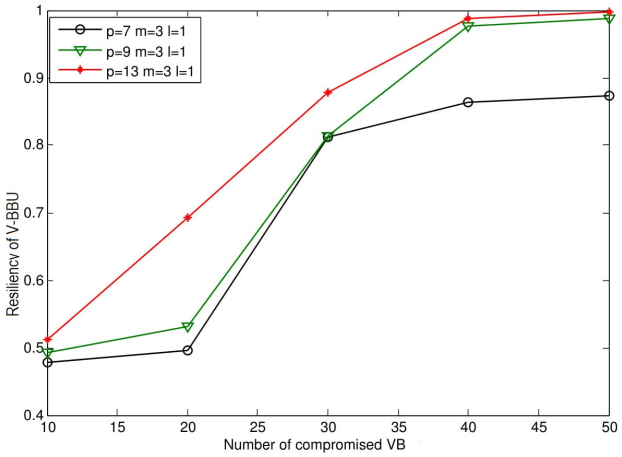

Fig. 4. Obtained Resiliency graph

B. Simulation for authentication process:

We have simulated the authentication protocol using is Automated Validation of Internet Security Protocols and Applications (AVISPA) tool in a Linux environment with system configuration of 8GB RAM with 64 bit OS [18]. The proposed protocol is simulated in two modes i.e. On-the-Fly-Mode Checker (OFMC) and the Constraint-Logic-based Attack Searcher (CL-Atse). In (OFMC), it visit the nodes by falsification and bounded verification by traversing through intermediate format (IF) specification in a demand-driven way in which it checks all role of the node and verify the session

Fig. 5. Simulation result of UE authentication in OFMC back end and CL-atSe back end of AVISPA tool

that is created with the help of node then it starts checking role by role and by taking all the possible attacks in the role module in which it visits 4600 nodes with a search time of 3.82. In Constraint-Logic-based Attack Searcher mode, each checker searched the node role by role and visited each node to check the possible attacks by using heuristics and redundancy elimination technique. The simulation checked 16691 nodes to find possible attack. The total time required to visit the nodes in o.13 second to check the possible attacks. The result shown in Fig 5. shows that proposed protocol is safe from the attacks that are discussed in the previous section .

VI. Conclusion

The use of cloud computing and virtualization technology for radio access network services is rapidly increasing. The rapid use of virtualization technology leads to more security challenge in the baseband unit of a C-RAN architecture. The independent operation of VB needs a secured key distribution strategy to maintain VB integrity and confidentiality. In this paper, we have described some key security challenge for the next-generation BBU-pool and provided corresponding solution to these challenges. The proposed protocol is secured and it efficiently assign the key to each authenticated VB in a V-BBU. The security protocol for V-BBU is analyzed using AVISPA tools and the result shows that the proposed methods is almost secured from different mention attacks.

References

[1] P. Demestichas, A. Georgakopoulos, D. Karvounas, K. Tsagkaris, V. Stavroulaki, J. Lu, C. Xiong, J. Yao, "5G on the Horizon: Key Challenges for the Radio-Access Network", *IEEE Vehicular Technology Magazine*, pp. 47-53, 2013.

[2] K. Chen, R. Duan, "C-RAN the road towards green RAN" , *China Mobile Research Institute, white paper*, 2011.

[3] J. Wu, J. Zhang, Y. Hong, and Y. Wen, " Cloud radio access network (C-RAN): a primer" , *IEEE Network*, pp.35-41, 2015.

[4] 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" , *4th International Conference on Recent Advances in Information Technology (RAIT)*, pp. 1-6, 2018.

[5] F. Tian, P. Zhang, and Z. Yan, " A Survey on C-RAN Security", *IEEE Access*, vol. 5, pp. 13372-13386, 2017.

[6] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," in IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 843-859, Second Quarter 2013.

[7] L. Eschenauer and D. G. Virgil , "A key-management scheme for distributed sensor networks", *ACM Conference on Computer and Communications Security*, pp. 41-47, 2002.

[8] S. K. Addya, and A. K. Turuk, "A technique for communication of distance node on key pre-distribution in wireless sensor networks", *ACEEE*, 2010.

[9] K. M. Martin, "On the applicability of combinatorial designs to key predistribution for wireless sensor networks", *International Conference on Coding and Cryptology. Springer,* 2009.

[10] D. R. Stinson, "Combinatorial designs: constructions and analysis" , *Sigact News*, vol.39(2), pp.17-21, 2008.

[11] D. Chakrabarti, S. Maitra, and B. Roy. "A key pre-distribution scheme for wireless sensor networks: merging blocks in combinatorial design" *International Journal of Information Security*, vol.5(2), pp.105-114, 2006

[12] D. Hyde, " A survey on the security of virtual machines" , *Dept. of Comp. Science, Washington Univ. in St. Louis, Tech. Rep*, 2009.

[13] K. Sonar, H. Upadhyay, " A survey: DDoS attack on Internet of Things" , *International Journal of Engineering Research and Development*, vol. 10(11), pp. 58-63, 2014.

[14] V. Varadharajan, U. Tupakula, " Security as a service model for cloud environment", *IEEE Transactions on network and Service management*, pp. 60-75, 2014

[15] Z. Yan, Zheng, Li. Xueyun, and R. Kantola. "Heterogeneous Data Access Control Based on Trust and Reputation in Mobile Cloud Computing." *Advances in Mobile Cloud Computing and Big Data in the 5G Era*, Springer, pp. 65-113, 2017.

[16] M. A. Iqbal, M. Bayoumi, "Secure End-to-End key establishment protocol for resource-constrained healthcare sensors in the co text of IoT" , *In High Performance Computing & Simulation (HPCS), International Conference* , pp. 523-530, 2016.

[17] S. Yu, C. Wang, K. Ren and W. Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," *Proceedings IEEE INFOCOM*, San Diego, CA, pp. 1-9, 2010,

[18] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. H. Drielsma, P. C. Hem, O. Kouchnarenko, J. Mantovani, S. Mdersheim, D. V. Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Vigan, L. Vigneron, " The AVISPA tool for the automated validation of internet security protocols and applications", *International conference on computer aided verification*, pp. 281-285, 2005.