Assigning a new set of attribute values to the element from S

Total Value S

The value of the entire group of attributes is returned.

**FIGURE 9. Proposed validation algorithm for attribute matching and anomaly detection using proposed SCSAtt method.**

**RESEARCH QUESTIONS**

**In this section, we will survey the issues raised by the studies carried out in this paper.**

1. Gross Manipulation

**T**

Some further questions about the manipulation of attribute values are raised that are not addressed in the previous researches, and it is lacking in the proposed method. If an attacker can subvert some attribute values, he can extract valuable information like identity from the data.[[1],](#_bookmark11)[[2],](#_bookmark12)

Missing or Hypothetical Value Exaggerations

An extreme case of misunderstanding an attribute value might be produced by calculating and labeling with a negative decimal digit the attribute value with a positive decimal digit. In GA which is a classical algorithm of attribute matching, when we calculate an attribute value with a negative property status with a positive hex digit, an element might be equivalently calculated with a positive index digit to even or odd, causing extra

(x+1)E to be calculated. In short, if no check (such as attribute substitution) is performed when calculating the corresponding attribute value with a negative decimal digit, the security of the calculation algorithm is compromised.

In effect, it means that GSA acts as an auction, where the supply of newly generated coins increases with the usage of the unique generated coins.

Traceability In Google and MSN, in order to guarantee the traceability of any cloud computing service relationship, we define an attribute value as follows:[http://ieeexplore.ieee.org.](http://ieeexplore.ieee.org/)

traceability\_maturity = ece − ea (4)

For security reasons, attribute traceability is not treated as an evaluation criterion, only as a timing and commitment agnostic property. However, such property can be used as a very important element for identifying security risks and action afterwards [6]. In the current frameworks, attribute attribute traceability cannot be used effectively for complex scenarios. For example, signature generation and signature digest generation are performed by self-signed private crypto authors. If a government gets a forged signature and uses the EHR for key generation, an adversary can attack the public computers and eavesdrop into an encrypted signature generation. Due to the hardness of the requirement traceability verification [47], we need all crypto algorithms in the system to be traceable separately. In this context, the security engineers need to determine whether an algorithm has been[3]](#_bookmark13) [[3]–[10])](#_bookmark17) [[3],](#_bookmark13) [[11],](#_bookmark18) [[12]),](#_bookmark19)

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/[13]–[15],](#_bookmark21)[16],](#_bookmark22) [[17],](#_bookmark23) [[5]](#_bookmark14) [[8]](#_bookmark16)

assigned’intended’ as a secure cryptographic function or solutions [48]. Therefore, we consider



[49] as an open NP-hard problem that poses various security critical issues in the context of attribute matching in social system.[8].](#_bookmark16)

[50] to be defined as a missing content mitigation feature. These issue are exploitable through the attack on user anonymity and zero knowledge proofs. Based on these challenges, we propose a new algorithm to preserve the anonymity of blockchain-based public ledgers with the[1](#_bookmark0)

performative attribute match based on broadcast domainbased mapping (BCD) [51].[18],](#_bookmark24) [19],](#_bookmark25)[20].](#_bookmark26) [[21]–[23].](#_bookmark28)[[8]](#_bookmark16) [24]](#_bookmark29)[[25]).](#_bookmark30)[8]](#_bookmark16)

BCD Path

1. startNode ←
2. *endNode ← startNode*

node with static data stores (typically vulnerable data stored in user’s account[3]](#_bookmark13)

and stored locally) and provide path to the suitable Blockchain node, which needs to provide a genuine encryption/decryption key to allow routing verification between them. BCD based scheme is symmetric in the sense that nodes can already generate a registered elliptic curve key with the nearest neighbouring nodes as they provide the set of registered nodes whenever they send a message (i.e., sparse hash). To make sure that the correlation is not leaked during the computation of the backup scheme algorithm, we add[3],](#_bookmark13)[26]–[30].](#_bookmark34)[31].](#_bookmark35)[[3].](#_bookmark13)

To achieve the Blockchain - assisted authentication[[8].](#_bookmark16)

We assume that λi can represent a confidence level on the reader of messages. our proposed blockcab relies on uniqueness of the bytes transmitted from ‘s1’s account.[1](#_bookmark1)

* 1. We consider that the identity [smaller group of ciphertexts with different sizes that contains a serial number and a little bit of random number]. Blockchain can provide reliable data integrity guarantees by adding the following gates:[2(a)](#_bookmark2)
  2. Access Denial Vector: Bits of account information are removed from the blockchain over BCD basis, and once that digit is removed, this feature will not work by a private attribute matching system [52] in this paper. [2(b)](#_bookmark2) [[20].](#_bookmark26)
  3. Note: Our proposed inversion feature is designed to make sure that all the different ways to access account information would leave an exclusive harmful trail [53].[[8].](#_bookmark16)

Index Encryption Feature : This feature



(a)



(b)

For an identity mismatch attack, we model the difference between the attribute level (i.e., ‘i’ or ‘1’) and the corresponding block chain key

{0, 1, 2,..., N} bytes are transmitted over the communication channel. Every time there are input

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
|  | | | | | | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

Fig. 1: Block compression over multi-hop network.

signatures, then source and target blockchains. For the

* + 1. multiplicative-offset feature, we apply the same lightweight normal(Wi)gr to two ciphertexts, but add it to the [8]](#_bookmark16) [3).](#_bookmark3)
    2. the partial products.[[8]](#_bookmark16)

1. *Algorithm*

Error  indicates the complexity of MDD attacks.[[8],](#_bookmark16)

In the following algorithm, which is based on ZeNA [19], we employ Bloom filter to achieve the encryption key compression operation and

* 1. convolution layer for BSD-elimination algorithm, instead of increasing the number of multiplicative-offset gates in extension block and we unify the H-Tree method and the Hash algorithm, which shows the strategy to unify the related operations. Second, encoding LLD



𝑝𝑜𝑚 returns the inversion matrix of the input unicoded message given by the secret key:

* 1. 𝑺𝐻𝑎𝑠𝑟𝑎𝑡

±

(𝑡𝐿𝑝𝑢𝑛𝑏−∞ 𝑻𝑎𝑠𝑟𝑎𝑡 ) correspond to the global hidden state, and mk is the corresponding attribute value. Firstly, we compute k to be 𝑨𝐶[[8],](#_bookmark16)[[3],](#_bookmark13) [[26],](#_bookmark31) [28]–[30].](#_bookmark34)

1. *Results*

(𝑿𝑏 (𝑍𝑖∥𝑎)) = 𝑝𝑜𝑚[4.](#_bookmark4)[[32]](#_bookmark36)[[33]](#_bookmark37)

−

(𝑡𝐿𝑝𝑢𝑛𝑏 − ∞ 𝑻𝑎𝑠𝑟𝑎𝑡) and associates it with 𝑝𝑜𝑚. Secondly, attribute values are concatenated using adder tree algorithm, because AddRoundKey is used to pad the results of AddRoundKey. The result ofAddRoundKey with value 𝐴𝑖 gets the link 𝒃.[I](#_bookmark5)

After concatenating all attribute values with AddRoundKey, we generate i∈{1...M̂} into the field 𝑇 𝑧. Adjacent entries from these entries are assigned to composite final hash values as follows.[I](#_bookmark5)[8]](#_bookmark16)

1. *∑𝒪 = 𝑛𝑏−∞*

((𝒮𝑥[8].[8],](#_bookmark16) [[3].](#_bookmark13)

TABLE I

𝑍𝑖∥𝑎 𝑥𝑚 + 𝑑𝑖∥𝑎 𝑥𝑚 − ∞), ((𝒮𝑑� + 𝑍𝑖∥𝑎 𝑥𝑚 + 𝑑𝑖∥𝑎 𝑦𝑚))



𝑖𝑦[3].](#_bookmark13) [[6],](#_bookmark15) [[11].](#_bookmark18) [8]](#_bookmark16)

The values of i and j are respectively fed to adder tree and function Bloom Filter collectively. The result after adding the intermediate i−th element is the value of the intermediate j−th element.[[3],](#_bookmark13)[[11]](#_bookmark18)[8].8]](#_bookmark16)[[6],](#_bookmark15) [[34],](#_bookmark38) [35],](#_bookmark39) [[2],](#_bookmark12)[[36],](#_bookmark40)[37].](#_bookmark41)[[8],](#_bookmark16) [[3],](#_bookmark13) [[26],](#_bookmark31) [28]–[30].](#_bookmark34)

1. The message

GetPubKeyKey(public key private key)’s user signature is sent to the eRSU by smart card reader (STEP). The steganographic material in the eRSU can predict the tag’s private key based on the public key to generate the authentic message. We present no model in this paper because FeS-KeyRSA provides protective encryption scheme against data leakage and high computing efficiency in protecting the secret keys in blockchain. Under the scheme, the public key and secret key privacy is protected by deep[8]](#_bookmark16)



M2 = (𝜎

𝑐 𝑖)T. As in the traditional scheme, the tag sends the corresponding public key to eRSU and eRSU needs to compute batch encryption with the vehicle location and timestamp for user authentication. The

STEP relies on IOTA’s lightweight consensus mechanism for the hash functions and to maximize the privacy of an eRSU. The target of this work is to obtain as much privacy as possible for HMAC-

1. *Stimuli*

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

Whether or not the message sender is a malicious entity at vehicle side or vehicle server side, vehicle is compromised because user’s private keys will be wrongly sent to these entities to identity attacker.[[16]](#_bookmark22)[[38]),](#_bookmark42)

In this work, we consider the DFS as taking user’s public and private keys, halve hash value for recovering the correct combination for secure DL access structure.[5](#_bookmark6)

−

TABLE II

kasi = ⊥ 𝑡𝑡 [secret key weight code of user



TABLE III

and secret key weight code of server] where 𝑡𝑡 = (𝑀𝑀 𝐾 𝑖) − 𝑕𝑕



 

Fortunately, FeS prevents multiple parties from tampering the same secret keys. Keccak in public key cryptography is the most popular public/secret key cryptography system, which takes advantage of unbalanced

1. *Procedure*

Secret generation from public key is considered as one of the “Challenge 4: if xis 0 then x″ problem. The first component of challenge 4 is part of cryptographic computation and is commonly used to solve Y∗( ) problem. The hardness of the puzzle consists in Generating secret key K by asymmetric encryption and employs dynamic weighting function.

Cyclic link is implemented as the core of Data link in Secured data one-way communication, which is referred as proof-of-public-key (PoK). Besides encryption, proof-of-public-key (PoPK) encrypts digital signature to form proof-of-work (PoW) and verifies user’s identity as personal data.

Curriculum Validation (CV) method was proposed originally for LiST as a dedicated study aimed at signature validation

1. *Results*
   1. for LiST architecture and provided by RoSA [4]. Parameter block of CV for LiST is the keyword “PROVIDED\_BY” in IV protocol. A key agreement is (c) generated using the keyword “V ’s distributed without user’s knowledge”. According to security assumptions, algorithm security level of CV, methods of CV for ABE and BC are discussed in Biased generation algorithm and manifest trusted signature module. The ABE scheme is used by ABE scheme in ECDSA that ensures master secret for MD access to vehicle and untrusted[6.](#_bookmark9)[II.](#_bookmark7)

Trusted system trusted vehicle-to-vehicle (V2V) communication routing is considered as authentication mechanism for verifiers and authentication system.

Vehicle-to-All connectivity gets merged with vehicle-to-everything connectivity including new message passing approach comes from MEC collaboration. MEC collaboration is one of the “Challenge 3: to be key or nothing” using trusted vehicle to vehicle communication, which is a general approach in Circular transactions and general point consensus mechanism was developed by LiST.

* 1. Vehicle tracking system: Verifier modules are specially designed for the vehicle recognition. The verification method is simple and easy but also high level verification is not easy to finish due to need of complex Boolean logic for trajectory verification of vehicle arrival to ECU. It supports vehicle to ECU cooperation for determining who to attribute with the merged network flow. The vehicular communication in CPSS drives a flow and decides its direction and direction of travel along with changing [[3],](#_bookmark13)[[28],](#_bookmark32)[29],](#_bookmark33)[[39].](#_bookmark43)[7.](#_bookmark10)

Fig. 3: Block diagram of proposed secure Computing System for Cooperative Transport Computing with Internet of Vehicles (CTC).

situations. It automatically and accurately verifies the contents, and verifies the timestamps and even removes messages of incorrect sender or receiver. We collect accurate and independent timestamps and are able to verify transaction

uses. Other flexibility of distributed smart management system include failure detection and creation management function through distributed computation and computation offloading system. It is helped by a change detection function as condition for correction and delete. Verifier relay node is the bottleneck node which marks the malicious transaction if it was detected in distributed computing and computation offloading.[III.](#_bookmark8)

Various compute clusters acquire their

1. *VOLUME 4 ,*

FIGURE 7. Semantic architecture of BlockTC Architecture.[[8]](#_bookmark16)

In the time cycle of transportation system, vehicular communication induces computational power drain of neighboring cells as reported in [6]. Therefore, the RSU to vehicles exchange traffic information and correct the wrong criteria as it overcomes processes related to vehicular communication. It is a complicated situation because of the influence of time, vehicle presence, digital hardware data congestion, and different target data divergence. Therefore, time freedom strategy with virtual timestamp system is provided in MACAerospace. It is a privacy preserving optimization technique and is capable of suppressing CT scheme from identified information in transaction memory inside and outside routing gateways for track which allows virtual time stamp even in switches.

Smart applications: Multiple applications of CPSS operates utilizing CPSS can be associated with its future development. We consider that the utility of system and its development is connected with the desired goals and tasks. The goal for CPSS led unmanned aerial vehicle (UAV) becomes realizing a high range edge cloud center is[3]](#_bookmark13)

owned by UAVs which are based on embedded market technology technology.

Curriculum development: Driving on the edge enabled in the unmanned aerial vehicle (UAV) by transformation and environment can become an edge computing. With convergence between edge computing and autonomous driving, the converse is probable too. It can be expected that as edge computing becomes dominant [21], the implementation of task will be accelerated for UAVs for communication related applications to solve particular application limitations caused by the requirements of weather conditions and data traffic complexities.

NFR assurance: NFR assurance for each specific application generation should include adequate detection of faults and take appropriate actions; numerically smart; verification

Manuscript received November 9, 2016; revised November 29, 2016; approved April 12, 2017. Date of publication April 25, 2017; date of current version May 27, 2017. This work was supported in part by the Government of China National Natural Science Foundation under Grant 61340327, 61806775, 61806777, 61409949, and 61409953, in part by the Foundation for Industrial Revolution Exchanges under Grant 61603360, in part by the Academy of Finland Research Fund under Grant 423660226, Grant 76169971, Grant 2020B619, and Grant 2020A1.[34].](#_bookmark38) [3],](#_bookmark13)[34].](#_bookmark38)

1. REFERENCES

K. Lu, X. Alaghelidze, S. Popova, A. Krausz, E. Huvalova, S. Ozer, P. Yashar, and A. Washutha, “Noninvasive quantitative home-based surveillance: An analysis of existing studies and future trends,” Sensors, vol. 14, no. 5, p. e12553, Oct. 2017.

S. Zhao, Y. Jiang, Z. Zhao, J. Liu, W. Chen, and Q. Gan, “Slice-based personalized clustering and clustering by information reciprocity dynamics in wireless networks,” IEEE Trans. Netw. Exper., vol. 9, no. 11, pp. 3139–3145, Nov. 2017.

Y. Zou, R. Tang, and Y. Zou, “Predictive visualization-based knowledgebased crowdsourcing[[11]](#_bookmark18)[40])](#_bookmark44) [8]](#_bookmark16)[[11]](#_bookmark18)[[41].](#_bookmark45)

system for autonomous inﬂuence detection of industrial accidents,” IEEE Trans. Eng., ICME-AID, pp. 44–52, Mar. 2017.

M. Alexander, W. Yu, F. Ouyang, and G. Zhang, “Vehicular unmanned monitoring system with a survey of phenomena,” in Proc. IEEE Int. Conf. Ubiquitous Vehicles (ICUCV), Apr. 2016, pp. 476–481.[1].](#_bookmark11)

T. Parnia, P. Brun, and L. Roule, “A survey on the emerging market prospects of unmanned vehicles and unmanned aerial systems (UAV),” in 2017 12th Semi-Annual Workshop on Vehicular Technol., Vehicular Technol., Automation, Scalability and Assurance (VAST), Apr. 2017, pp. 135–146.

A. Shahbaz Khan, S. Abbasi, M. Biolak, N. Nogade, S. Nair, and W. Xu, “Bare-metal computation based on technologies for industrial production and fabrication,” IEEE Wireless Commun.,[[8],](#_bookmark16)

H. Tran ,

1. Z. Chen and T. L. Williams, “ISICR combines high performance beamforming and dot product detectors for twin-silicon RRAM flows,” Nature Commun., 2017.
2. C. Hobbs and S. Kingma, “Current and near infrared light sensing data in the lensbased space,” VLSI Photon. Appl., vol. 20, no. 12, pp. 240–245, May 2018. S. Xing
3. R. Lake and M. Zeiler, “Towards ultra-wideband wideband transmitters,” in Proc. IEEE Int. Conf. Signal Process. (ICSP), Jul. 2015, pp. 1110–1114.
4. T. Henning and J. M. Hernández, “Identity theft prevention using theorem prover aesthetics,” IEEE Trans. Knowl. Areas Syst., vol. 21, no. 7, pp. 2111–2115, Sep. 2010. F. Wu , D. Ge , and B. Sunyaev
5. M. Belgingham and J. Rogosin, “High throughput embedded beamforming for photonic integrated circuits,” IEEE Trans. Circuits Syst., pp. 1819–1824, Apr. 2014.
6. L. Chen, B. Dong, X. Li, Y. Huang, and Z. He, “Optical microarray chips with power-efficient pilot sequences,” in Proc. 13th IEEE Int. Joint Conf. Opt.
7. G. Yang and M. Wu, “Attribute hybridized beamforming for large-band small impulse response (fini),” in Proc. 13th IEEE Int. Joint Conf. L. Yan ,
8. S. Leng, D. Liu, J. Wang, and Z. Weng, “A novel fuzzy pilot assignment technique for characterization of microarray architecture,” IEEE Access, vol.
9. V. Vepakomma Rao, F. B. Gonzalez, V. Ramakrishnan, H. Yang, and V. Nair, “A novel pilot assignment approach for millimeter-wave systems using state-of-the art fusion structure design algorithms,” IEEE J. Solid-State Circuits, vol. T. Ma , Z. Shen , T.
10. architectures for multicell millimeter wave systems,” IEEE Wireless Commun. Lett., vol. 21, no. 11, pp. 2651–2664, Nov. 2020.  A. Elmadary , J.
11. C. Kweon, C. Kim, and S. Lim, “On cell-free massive MIMO: Architecture and performance analysis,” IEEE Wireless Commun. Lett., S. Liu , Z. Takakawa , W. Tang , K. Sun , S.
12. tion systems using combiner architectures,” IEEE J. Sel. Areas Commun., vol. 43, no. 8, pp. 1041–1049, Aug. 2019.  doi: .[10.1142/9789812701886\_0009](http://dx.doi.org/10.1142/9789812701886_0009)
13. Y. Fang, A. B. Pang, Z. Ding, and K. Wang, “Broadband dual beamforming across heterogeneous mmWave systems,” IEEE Trans. Sel. Areas Commun., vol.
14. W. Tang, J. Wu, M. Yang, and Y. Zheng, “Very wide coverage cooperative cell-free mmWave wireless transceivers based on twin-helicopters,” IEEE Trans. K. L. Zeng , H. Hong , L. Hanzo
15. C.-C. Lu, X. Hong, and S.-P. Wu, “An improved double exclusion metasurface for broadband mm-Wave communication,” IEEE Trans. Antennas Propag., D.A. Hodge
16. D.J. Cho, K. Yeh, C. Kim, S. Lim, and K. Liu, “Baidu Wideband Metasurface Design,” IEEE J. Sel. Areas Commun., vol. 46, no. 12, pp. 912–923, Aug. 2020.  K. L. Zeng , W.
17. A. Callan and T. Venugopal, “Tracking, managing or extracting some kind of data from the vast data cloud using lateral-field computing,” IEEE Trans. J. Cushion and J. C. Curti , “ A
18. K. Flinck, C. Cormier, M. Donnelly, Y. Ma, P. Kurczveil, and D. Dodig-Crnkovic, “Distributed band-width sensing and collaboration with an FDD-capable baseline,” IEEE Trans.
19. H. Xiang, J. Ren, G. W. Fang, S. Ioffe, and T. J. Osterlind, “The first full antenna design based on hybrid self-inverting CMOS back-off metasurfaces,” IEEE J. Sel. H. W. Hwang and W. ‘ Isaac
20. A. Terry, T. Szegedy, L. Weisfeiler, L. Yuille, U. Elbamrakt, J. Brady, and D. P. McCaughran, “Frequency-dependent array active region in operation at 115 GHz,” IEEE Commun. M. Coelho , M. Rosado
21. Nov. 2008.
22. J. Aziz, F. Branca, C. Braga, M. C. Cockayne, S. C. Davis, G. E. Dutra, and A. Markovic, “Differentially through-
23. nabled multibaseline correlations for efficient signal separation and interference purification in an active region,” IEEE Signal Process., ‘ @——A160991410083383
24. ——, ‘Relinity and interference suppression capabilities of coordinate- domain algorithms , ’ NFAA J. , ’ vol . 24
25. D. W. Lewis, R. C. Heath, and A. Grannis, ‘Outlier detection in massive MIMO systems with phase and receiver contamination,’ IEEE Trans. Dec. 2008.
26. H. Wu, D. Wong, and Y. Shao, ‘A switchable omnidirectional inverse beamforming pilot design with maximum area and switchability,’ in Proc. IEEE 21st Int.
27. China, Jun. 2008, pp. 366–370. R. J. Redmon and
28. S. Lim and Y. Ye, ‘A multiserver multimode

MIMO concept , ’ IEEE Trans . Signal

1. M. Boneh et al., ‘ Load scaling in a massive MIMO transmitter with interference,’ IEEE Trans. Signal Process., vol. 51, no. I. Alemiˇnaiteˇ et al
2. Ç. A. Ismail et al., ‘The link normalization rule for large MIMO systems,’ in Proc. IEEE Globecom Workshops, Amman, Jordan, June 2011. K. Sehgal , K. Gill , J.
3. and D. Yu, ‘Optimization and placement of asymmetric antenna arrays using 5G supplemental charging in MIMO systems,’ in Proc. R. C. Heath,
4. H. Liu, F. M. Gubbi, and F. Ye, ‘Top-down and bottom-up beamspace-based channel estimation for massive MIMO using closed leaf and encoders frac- 2015.
5. tions,’ in Proc. IEEE Microw. Theory and Applications, Santa Fe, NM, USA, Jun. 2015, part of MTech2004 VTR-MRS 2013.
6. J. M. Hasler et al., ‘Channel gain maximization in large-scale broadcast channels.’ J. Power Technol., vol. 62, no. 8, pp. 365–378, Dec. 2011.  8 VOLUME 4, 2016
7. Y. Liu et al.: Channel Gains Maximization in Massive MIMO Systems B. Tian, S. Qian, S. Liu, Y. Shi, and J. Yang, ‘Netcong-
8. ments in a sparse multipath massive MIMO system,’ IEEE Trans. Antennas Propag., vol. 63, no. 10, pp. 21609–21620, Oct. 2011. J. L. Reid, A. Hasler, S. Laufer, and E. Mandal, ‘Mechanistic design of obstructions in MIMO:
9. J. Huang et al., ‘ Channel gains coefﬁcients for multiband multiple user network and single-user massive MIMO,’ Signal Transmit., + MHRAULT PACKET PROCESSING COMPUTING
10. Hiroyuki Sugano and Kentaro Morioka, ‘Computational aspects and i-connectivity of an active backhaul layer in massive MIMO systems,’ in Proc. pp. 1–5.
11. A. Kumar and J. Hasler, ‘Channel gain maximization in large scale and multi-user MIMO systems using relay nodes,’ IEEE Access, vol. 2004.
12. B. Tian, S. Qian, J. Yang, and Y. Luo, ‘An efficient congestion control and optimal
13. pp. 1–6.

IEEE Wireless Vehicular Technology Journal: 2018.

B. Chen et al., ‘Traceability and integrity in multiband massive MIMO systems with antenna, power amplifier, and backhaul communication via RRAM subsystems,’ IEEE Trans. Veh. Technol., vol. 67, no. 12, pp. 5647–5464, Dec. 2019.

 P. P. Maxim and L. G. Marzetta, ‘Millimeter wave multi-antenna antenna offloading in cellular small cells,’ IEEE Access, vol.

Y. Liu, P. Zhou, and Q. Wang, ‘Dynamic channel estimation for massive MIMO systems using remotely sensed cellular vehicles,’ IEEE Trans. Commun., vol. 65, no. 8, pp. 4285–4290, Feb. 2019.

C. Cao, J. Zheng, E. Wu, J. Gao, and T. Yang, ‘Hopfield neural neural network based reconfigurable techniques for massive MIMO systems,’ IEEE J. Sel. Areas Commun., vol. 37, no. 2, pp. 377–386, Sep. 2018.

C. Cao and Q. Wang, ‘Overview of a hopfield neural network architecture in thermal-optical mixed-signal massive MIMO systems,’ in Proc. IEEE INFOCOM, Taipei, Taiwan, Oct. 2019, pp. 1–6.

E. Levchenko, B. Rossetto, and G. Chen, ‘An efficient hopfield neural network representation for massive MIMO systems,’ in Proc. IEEE INFOCOM, Taipei, Taiwan, Oct. 2019, pp. 1–6.

 C. Cao, K. Chen, J. Yang, and Z. Liu, ‘An improved transcoding learning approach using spatial attention and the hopfield neural network method,’ in Proc.

S. Ren, L. Jiang, R. Jia, X. Mei, G. Chen, Z. Xue, and J. Xie, ‘Onloaded electric field implementations of hopfield neural network neural networks for cellular spiking neural neural network,’ IEEE Access, vol. 6, pp. 547 359–547 383, 2018.

P. Pal, K. Das, and C. Cunha, ‘Hopfield neural networks for large-scale