Lightweight Authentication Protocol for Inter Base Station Communication in Heterogeneous Networks

Gaurang Bansal and Vinay Chamola
Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani Campus, India.

***Abstract*—Over the past few years, with increasing mobile traffic and decreasing revenue per user, Heterogeneous Networks (HetNets) have become a topic of interest to many stakeholders. HetNets is a combination of networks with different access technologies and cell types working with each other. Mobile network operators are keen to reduce operational expenses by deploying HetNets while they provide better QoS to the user anywhere, anytime wireless connectivity. Although HetNets provide various benefits, yet many open issues need to be addressed to harness their impact. They are also prone to several security threats such as physical attacks, man-in-the-middle (MITM) attacks, impersonation attacks, replay attacks, and node tampering attacks. Moreover, due to the different nature and structure of each network in a HetNet, secure handover between various wireless networks is a complex task that is not yet resolved. In this paper, we address the issues mentioned above by designing a secure handover mechanism that is resistant to both passive and active attacks. We also show a performance comparison of our protocol with the state-of-the-art protocols for securing hetnets based on computation, communication, and memory storage cost.**

I. Introduction

HetNets is an emerging concept which brings various opportunities for cellular operators to reduce the operational expenses and to improve the QoS offered to the users. Although such networks have several advantages, safety and privacy problems stay major weaknesses [1] in their operations. System model for communication among base stations is presented in fig. 1. During the communication between a small base station (SBS) and a macro base station (MBS), much data is passed. However, an opponent could compromise this information flow by manipulating it or capturing it. This could lead to unjust or oppressive communication between the two sides. Also, the victim's data (which could be recorded) can be used in criminal operations and directed advertisements. The computing systems used in SBS are cheap, tiny, and affordable [2]. The SBS is very often installed in easily accessible locations. This allows an attacker to capture SBS units without being noticed. Hence, making SBS units safe against physical invasions is essential. An intruder, for example, could obtain and launch numerous exploits with the secret keys present on the unit. Physical Unclonable Functions (PUFs) have surfaced as a lucrative approach for defense against physical attacks. PUFs eliminate the need to hold private keys in the storage of the units and operate on challenging-response combinations. A PUF's challenge-response system captures the intrinsic variability of the IC fabrication process [3, 4]. Its response depends on both the input and the chip's physical microstructure [5]. The physical randomness induced by the variations in the manufacturing process helps to make each PUF unique, i.e., it is impossible to create two identical copies.

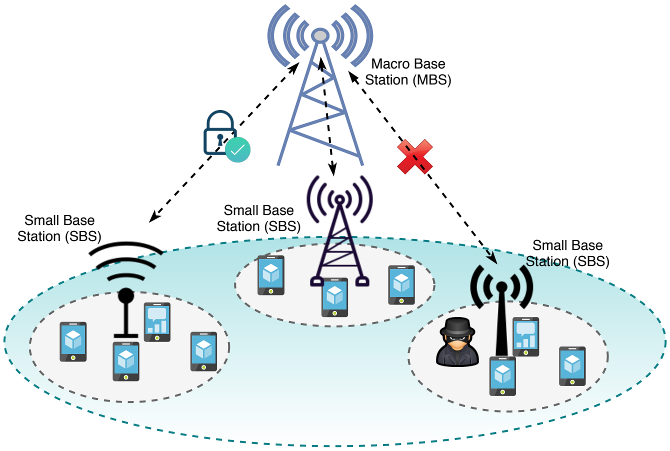

Fig. 1: System model

The rest of the paper is arranged as follows. The related work in Hetnets is discussed in Section II. Section III discusses a preliminary background of PUFs. Section IV details the network model. The Mutual authentication protocol is discussed in Section V. A Cryptanalysis is presented in Section VI. We evaluate and contrast the performance of our protocol with state-of-the-art protocols in Section VI and finally conclude the document in Section VII.

II. Related Works

As discussed in the Introduction, the open issues that need to be resolved for better deployment of Hetnets are primarily security threats and lack of easy handover mechanism. The Third Generation Project (3GPP) [6] in 2003, provided a specific key hierarchy for different wireless scenarios to decrease the amount of latency incurred in the authentication. However, this technique is not suited for 5G Hetnets because of heterogeneity among networks; it increases the complexity of authentication. Moreover, it leaves the danger of secret keys being exposed in case of a physical attack on AP. Authors in [7] used remote server authentication among different network cells. As the number of inquiries from small MBS (SBS) increases, user verification is required each time, resulting in a latency of hundreds of milliseconds, which is unacceptable for 5G. Moreira [8] proposed direct authentication between a small MBS and macro base using public-key encryption, which involved a three-way handshake. Although the handover authentication procedure is simplified, computation cost and delay are increased due to the overhead for exchanging more cryptographic messages through a wireless interface [9, 10]. For the same reason, digital signature-based authentication is also a not viable solution for heterogeneous networks. Related work in [11] proposed a handover using user-assistance. In the paper, the current base cell transfers a signed authentication certificate as a context to the user, which user relays to target SBS. The problem with this architecture is that mobile is actively involved in handover authentication, which is not always feasible. Secondly, mutual trust between SBS and mobile devices is assumed in these solutions, which could be infeasible for 5G HetNets [12, 13].

None of those papers [14, 15, 16, 17] have taken physical security into account. Moreover, the proposed solution either compromise with security or the latency and computation cost. Therefore, there is a requirement of a secure and lightweight authentication mechanism in 5G networks.

III. Preliminary Background

PUF or Physically Unclonable function is something similar to fingerprint in human. It is biometric design of an hardware which uses hardware characteristics of an device. The distinguishing the attribute of a PUF is that it relies on a physical basis, making it impossible to reproduce a PUF using cryptographic primitives. Additionally, the term ”physical unclonable” indicates that it is computationally infeasible or difficult to produce a physically identical PUF [18]. By using PUFs in an interconnected system such as IoT or SBS systems, every single the device can have its own unique ”fingerprint” which cannot be cloned or reproduced. A PUF behaves like a mathematical function whose input (challenge) and output (response) are both in the form of a string of bits. A PUF function can be represented as:

$$K = PUF(C) \tag{1}$$

where the challenge C is given as input and response, K is the corresponding output to that challenge.

IV. System Model

The system model consists of three entities, namely legitimate small network cells or base stations (SBS), eavesdropper SBSs (attacked by a malicious entity and is compromised), and a macro MBS (MBS). Macro MBS is connected to the authentication server.

SBSs have limited memory and computational capability as compared to the MBS. In this model, multiple SBSs may be connected to a single MBS. SBS is equipped with a PUF, which is used for generating a response for a challenge input to it. The SBS itself does not store any secret keys. Instead, it performs a key expansion on the generated response to help create session keys.

Whenever a new SBS wants to register itself with the MBS, it's challenge-response pair (C, R) is securely sent and stored in the MBS. The MBS is the only trusted authority in this network, and therefore (C, R) pairs for all SBSs are stored only in the MBS. Further, in this model, for each SBS, the MBS starts with a single initial (C, R) pair, which it acquires at the time of SBS registration. After this initial exchange, the SBS can function independently without needing any technical personnel or any secure channel. While the SBS generates (C, R) pairs on the fly upon each authentication attempt, the new (C, R) pair is securely sent and stored in the MBS. [19]

A. Attack Model

We assume the standard attack model as used in [20, 21]

V. Proposed Protocol

In fig. 2, SBS initiates the authentication to MBS. It sends its ID, in here U_1 and a nonce N_A sends message to MBS B_1. The entities follow one time registration policy. All the authenticated SBS are once registered

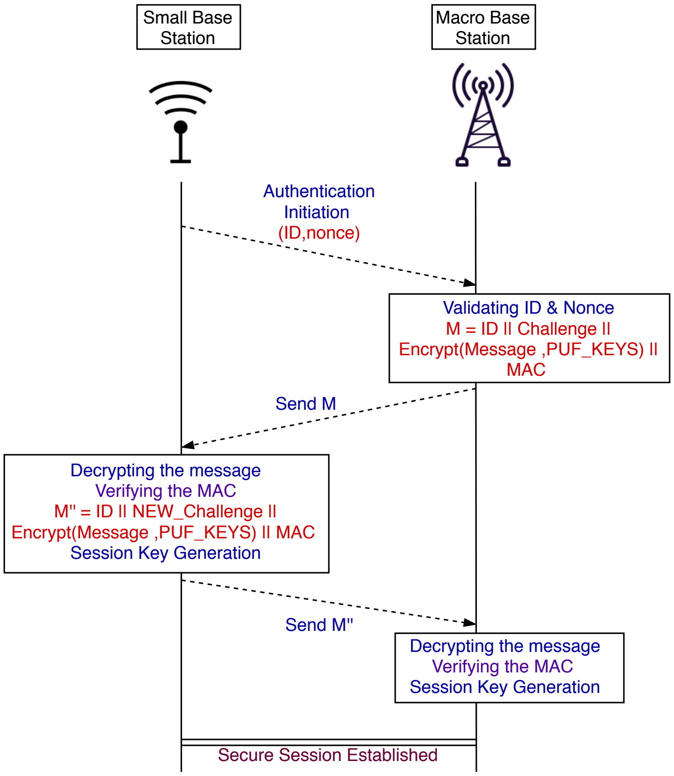

Fig. 2: Proposed Protocol

to MBS. This registration process includes storing of CRP pair in MBS. The entities are authenticated using the following protocol. This protocol ensures that only trusted SBS can authenticate with the MBS before they can begin any communication channels with the MBS. In this process of authentication, a secure session key is established between the SBS and the MBS, which can be used for further communication.

SBS U_1 wants to authenticate with a nearby MBS B_1, it sends its ID U_1 and a nonce N_A. B_1 checks within its database if U_1 exists and whether nonce N_A is fresh, i.e., it should not match the N_A generated in the previous authentication. If either of the condition fails, the authentication fails. The authentication failure because of nonce can help prevent replay attack. In replay attacks its possible that an adversary may store previous communication and use the information send by trusted SBS to authenticate itself. B_1 finds the corresponding challenge-response pair (C, R) from its database. This database stores the CRP during the one time registration process as discussed before.

Security increases with increase confusion and diffusion. Confusion and Diffusion can be increases by increasing the Key size. Since the devices are memory constraint its not advisable to store multiple keys. Take for instance, there are 1000 SBS and each having 32 Key pairs. It would take around 32000 MB or around 32 GB of space. This is infeasible for any IoT device to handle such large volume of data. So we use a key expansion algorithm. Key expansion algorithm takes bits from diff combination and use to generate multiple keys. Elaborate describtion of key expansion algorithm is given in [22, 23]. Using one key it generate 16 keys $K_1, K_2, K_3, ..., K_{16}$ from the response R of the challenge-response pair (C, R). The MBS B_1 then generates a 32-bit nonce N_B, which along with N_A is the information to be encrypted, as $N_A||N_B$. δ is constant bit size concatenated with non linear output of F to match the size in XOR operation.

In here symbols are used as following:

- $A \longleftarrow B + C \implies A = B + C$
- $A||B \implies AB$
- $A \veebar B \implies A$ XOR B

$$
\begin{gathered}
X_1 \longleftarrow N_A \veebar K_{16} \\
Y_2 \longleftarrow N_B \veebar \delta||F\left(X_1\right) \veebar K_{15} \\
X_3 \longleftarrow X_1 \veebar \delta||F\left(Y_2\right) \veebar K_{14} \\
Y_4 \longleftarrow Y_2 \veebar \delta||F\left(X_3\right) \veebar K_{13} \\
\ldots \\
Y_{14} \longleftarrow Y_{m-4} \veebar \delta||F\left(X_{13}\right) \veebar K_3 \\
X_{15} \longleftarrow X_{13} \veebar \delta||F\left(Y_{14}\right) \veebar K_2 \\
Y_{16} \longleftarrow Y_{14} \veebar K_1
\end{gathered}
$$

The final cipher-text Q to be sent to U_1

$$
Q \longleftarrow (Y_{16} \| X_{15}) \veebar (K_{16} \| K_{15})
$$

B_1 then sends message C, Q and a MAC $MAC(B_1 \| Q \| N_A \| N_B)$ to U_1. MAC also known as Message Authentication Code is used for Integrity check. It is one way function that uses hash function. The idea behind is that it is one way function. The verifier can verify if the data it has got is right or not. An adverseary cant forge the MAC It is based on SHA 256. Within the MAC, the first parameter verifies the identity of the MBS, while data integrity is ensured by the second and third parameters. Freshness of the source (B_1 in this case) is identified by the last two parameter N_A and N_B.

On receiving the message from the MBS, U_1 generates the response R by passing the received challenge C through the PUF as given in (2).

$$R = PUF(C) \tag{2}$$

$$(Y_{16}||X_{15}) \longleftarrow (K_{16}||K_{15}) \veebar Q \tag{3}$$

This is divided into two 32-bit strings to get Y_m and X_{15}. The decryption procedure is identical to the encryption procedure, as can be seen in the following set of equations.

$$\begin{gathered}
L_1 \longleftarrow Y_{16} \veebar K_{16} \\
T_2 \longleftarrow X_{15} \veebar \delta||F\left(L_1\right) \veebar K_{15} \\
L_3 \longleftarrow L_1 \veebar \delta||F\left(T_2\right) \veebar K_{14} \\
T_4 \longleftarrow T_2 \veebar \delta||F\left(L_3\right) \veebar K_{13} \\
\cdots \\
T_{14} \longleftarrow T_{m-4} \veebar \delta||F\left(L_{13}\right) \veebar K_3 \\
L_{15} \longleftarrow L_{13} \veebar \delta||F\left(T_{14}\right) \veebar K_2 \\
T_{16} \longleftarrow T_{14} \veebar K_1
\end{gathered}$$

If verified, a new 32-bit challenge-response pair (C', R') is generated by U_1 using its PUF. It also generates a new Nonce N_C. This newly generated information is encoded into $M', M'' and N'$ as follows.

$$\begin{gathered}
M' \longleftarrow C' \veebar K_2 \\
M'' \longleftarrow R' \veebar K_3 \\
N' \longleftarrow N'_C \veebar K_4
\end{gathered}$$

The session key Ses_k with which further communication will take place is computed, as shown below.

$$Ses_k \longleftarrow ((F(K_5 \veebar N_B) \veebar F(K_6 \veebar N_C)) \tag{4}$$

M', M'', N' and a new MAC with five parameters is sent to B_1. B_1 calculates C', R', N_C and Ses_k as shown in the following equations.

$$\begin{gathered}
C' \longleftarrow M' \veebar K_2 \\
R' \longleftarrow M'' \veebar K_3 \\
N'_C \longleftarrow N' \veebar K_4 \\
Ses_k \longleftarrow ((F(K_5 \veebar N_B) \veebar F(K_6 \veebar N_C))
\end{gathered}$$

Now, B_1 has all the parameters to verify MAC. If the verification fails, authentication is terminated by B_1. If verified, it stores the new 32-bit challenge-response pair (C', R') for SBS U_1 in its memory replacing the previous entry (C, R). Thus, mutual authentication has been achieved. Both U_1 and B_1 compute the new Alias ID (AID) for U_1 and update it in their storage.

$$AID \longleftarrow H(U_1||K_7) \tag{5}$$

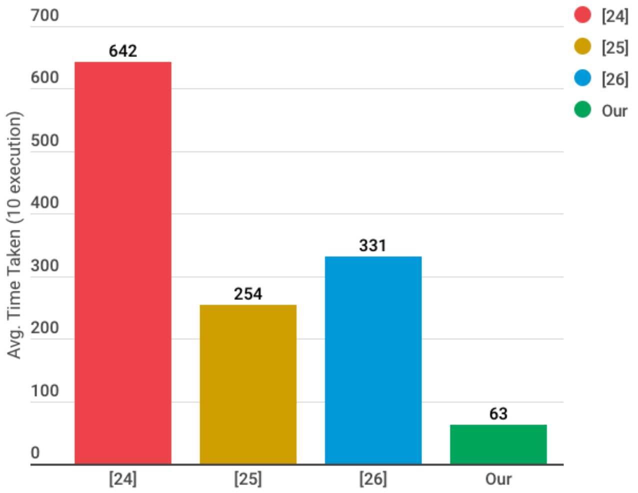

Fig. 3: Performance comparison of the proposed protocol with state-of-the-art schemes

Changing the ID of the SBS using a suitable hash function as shown in equation (5) ensures untraceability. An adversary will not be able to match the AID with any previous IDs.

VI. Comparison of Computational Performance

Here we compare the performance of our protocol with the protocols of [24], [25] and [26]. Fig. 3 shows the comparison of our protocol with the schemes mentioned above in terms of time consumed in various cryptographic operations such as Encryption/Decryption, Hash, MAC, Exponent, and Pseudo-Random Number Generation (PRNG). The simulations were run in Python 2.7 language on a 2016 MacBook Air with Core i5-5200U and 8GB DDR3 RAM. The protocols of [24], [25] and [26] respectively consume 642, 254 and 331 ms while our protocol consumes only 63 ms in these cryptographic operations for 10 executions of protocol. Thus, the proposed protocol is much faster than current state-of-the-art schemes.

VII. Conclusions

In this paper author present the problems in current hetnet communication. Although Hetnets are becoming popular yet there are many security issues that need to be resolved before its mass scale application. The paper proposes a lightweight mutual authentication protocol for SBS and MBS communication using physically unclonable functions (PUFs). The protocol uses a challenge-response scheme enabled by PUFs, which gives it the advantage of not having to store any secret information in the SBS nodes. Only one challenge-response pair per

SBS is stored in the MBS at a time. Finally we show the protocol is secure and computationally less complex in comparison to previous state of art techniques.

VIII. Acknowledgement

This work is supported by DST-SERB (Science and Engineering Research Board (SERB)) funding under Project Grant File no. ECR/2018/001479.

References

[1] H. Wang, B. Qin, Q. Wu, L. Xu, and J. Domingo-Ferrer, "Tpp: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2340–2351, 2015.

[2] A. Abdallah and X. Shen, "Lightweight Security and Privacy-Preserving Scheme for V2G Connection," in *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, dec, pp. 1–7.

[3] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," in *2008 IEEE International Conference on RFID*. IEEE, apr, pp. 58–64.

[4] A. Miglani, N. Kumar, V. Chamola, and S. Zeadally, "Blockchain for internet of energy management: Review, solutions, and challenges," *Computer Communications*, 2020.

[5] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Brand and IP protection with physical unclonable functions," in *2008 IEEE International Symposium on Circuits and Systems*. IEEE, may, pp. 3186–3189.

[6] K. Ahmavaara, H. Haverinen, and R. Pichna, "Interworking architecture between 3gpp and wlan systems," *IEEE Communications Magazine*, vol. 41, no. 11, pp. 74–81, 2003.

[7] X. Duan and X. Wang, "Authentication handover and privacy protection in 5g hetnets using software-defined networking," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 28–35, 2015.

[8] C. M. Moreira, G. Kaddoum, and E. Bou-Harb, "Cross-layer authentication protocol design for ultra-dense 5g hetnets," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–7.

[9] Y. Zhang, R. Deng, E. Bertino, and D. Zheng, "Robust and universal seamless handover authentication in 5g hetnets," *IEEE Transactions on Dependable and Secure Computing*, 2019.

[10] A. Jindal, G. S. Aujla, N. Kumar, R. Chaudhary, M. S. Obaidat, and I. You, "Sedative: Sdn-enabled deep learning architecture for network traffic control in vehicular cyber-physical systems," *IEEE Network*, vol. 32, no. 6, pp. 66–73, 2018.

[11] G. S. Aujla, R. Chaudhary, N. Kumar, J. J. Rodrigues, and A. Vinel, "Data offloading in 5g-enabled software-defined vehicular networks: A stackelberg-game-based approach," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 100–108, 2017.

[12] G. Bansal, N. Naren, V. Chamola, B. Sikdar, N. Kumar, and M. Guizani, "Lightweight mutual authentication protocol for v2g using puf," *IEEE Transactions on Vehicular Technology*, 2020.

[13] G. Bansal, N. Naren, and V. Chamola, "Rama: Real-time automobile mutual authentication protocol using puf," in *Proceedings of IEEE International Conference on Information Networking (ICOIN), Barcelona, Spain*. IEEE, 2020.

[14] V. Hassija, V. Chamola, G. Han, J. Rodrigues, and M. Guizani, "Dagiov: A framework for vehicle to vehicle communication using directed acyclic graph and game theory," *IEEE Transactions on Vehicular Technology*, 2020.

[15] V. Hassija, G. Bansal, V. Chamola, V. Saxena, and B. Sikdar, "Blockcom: A blockchain based commerce model for smart communities using auction mechanism," in *IEEE International Conference on Communications, Shanghai, China*. IEEE, 2019, pp. 1–6.

[16] G. Bansal, A. Dua, G. S. Aujla, M. Singh, and N. Kumar, "Smartchain: a smart and scalable blockchain consortium for smart grid systems," in *2019 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2019, pp. 1–6.

[17] V. Hassija, V. Saxena, and V. Chamola, "Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory," *Computer Communications*, vol. 149, pp. 51–61, 2020.

[18] Q. Chen, G. Csaba, P. Lugli, U. Schlichtmann, and U. Ruhrmair, "The Bistable Ring PUF: A new architecture for strong Physical Unclonable Functions," in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*. IEEE, jun, pp. 134–141.

[19] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R.

Choo, “Consumer iot: Security vulnerability case studies and solutions,” *IEEE Consum. Electron*, vol. 9, pp. 6–14, 2019.

[20] I. Butun, P. Österberg, and H. Song, “Security of the internet of things: vulnerabilities, attacks and countermeasures,” *IEEE Communications Surveys & Tutorials*, 2019.

[21] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, “Applications of blockchain in unmanned aerial vehicles: A review,” *Vehicular Communications*, p. 100249, 2020.

[22] T. Nie, C. Song, and X. Zhi, “Performance evaluation of des and blowfish algorithms,” in *2010 International Conference on Biomedical Engineering and Computer Science*. IEEE, 2010, pp. 1–4.

[23] R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, “Lattice based public key cryptosystem for internet of things environment: Challenges and solutions,” *IEEE Internet of Things Journal*, 2018.

[24] Z. Yang, S. Yu, W. Lou, and C. Liu, “P^{2}: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid,” *IEEE Transactions on Smart Grid*, no. 4, pp. 697–706, dec.

[25] N. Saxena and B. J. Choi, “Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1438–1452, jul 2016.

[26] H. Liu, H. Ning, Y. Zhang, and L. T. Yang, “Aggregated-proofs based privacy-preserving authentication for V2G networks in the smart grid,” *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1722–1733, 2012.