Novel Framework for Secure Handover Authentication Protocol for 5G Mobile Network

M. Said Abdelhady, W. Anis, A. Abd-Elhafez, H. Eldemerdash, Amr Abdelaziz

Abstract: This paper presents a comprehensive solution for secret key generation and user authentication for 5G mobile networks. Our solution exploits the integration between physical layer and cryptographic security primitives. The presented secure secret key generation and authentication protocol based on exploiting physical layer attributes Angle of Arrival (AoA) and merges between cryptography and non-cryptography techniques (physical layer security) to obtain secure and fast handover in 5G mobile network. Huge increasing of the exchanging data and the lack of the current usable spectrum (several hundred megahertz and a few gigahertz) led to the adoption of millimeter wave (mmWave) 5G mobile networks. The opportunity of the un usable spectrum in the millimeter wave (mmwave) range from 30~300 GHz mandates the utility of small cells with base stations (BS) equipped with large numbers of antennas massive Multiple Input Multiple Output (MIMO). This new architecture achieves better spectral and energy efficiencies, meanwhile, it also brings new challenges in security provisioning and new stringent latency requirements and potential risk of some security attacks. Impersonation and man-in-the-middle (MitM) attacks are examples of security vulnerabilities originated from the probable recurrent handovers and authentication processes in small cells architecture and Heterogeneous Networks (HetNets). The assessment and simulation for the proposed protocol has been proved using AVISPA tool against (MitM) attack and MATLAB tool against impersonation attack. The proposed protocol has the ability to mitigate these attacks with no extra communications overhead, yet, with tolerable delay of estimation process.

Keywords: Angle of Arrival (AoA), 5G security, multiple signal classifier (MUSIC), Transmission Encryption Key (TEK), man-in-the-middle (MitM).

I. INTRODUCTION

5TH generation mobile network, is the next generation after the existing (LTE) mobile network [1, 2]. The extremely growth of data traffic with new requirements, applications and insufficiency in available spectrum, where The relatively narrow available frequency bands between several hundred MHz's and a few GHz's have been almost exploited by unlicensed and licensed networks, including LTE-Advanced and all former mobile networks generations in addition to Wi-Fi. Or lead to intensive research and more development efforts on 5G mobile.

Also dynamic spectrum allocation could give some enhancement, the usable spectrum still not enough.

The solution is to find new spectrum for 5G by exploiting idle one in the millimeter wave range 30~300 GHz. This will lead 5G network to confront more difficult requirements and security challenges than former generations.

5G network will be depended on heterogeneous architecture with expansion in using small cells and its BSs will be equipped with massive (MIMO) antennas.

The expansion in using small cells in heterogeneous networks due to using mm-wave spectrum and massive (MIMO) antenna arrays will led to new challenges in network resources management and security requirements, like frequent handovers due to the mobility of users between ultra-dense small cells, which will lead to additional latency and increases the potential risk of some attacks like impersonation and (MitM) attacks.

Secure and fast handover is the main concern in this paper.

This paper will present novel framework for secure secret key generation and authentication protocol based on physical layer attributes (AoA) [3-6], for fast and secure handover authentication process in 5G mobile network.

Our protocol depends on two phases in the handover authentication process. Estimated (AoA) will be used to generate a truly random key conducted with conventional challenge-response authentication protocol, as a first phase in the handover authentication process. While the second phase will be the usage of estimated (AoA) as a fingerprint to the user equipment (UE) to be considered as a legitimate user in handover authentication process.

Estimated (AOA) calculated without extra communication overhead where the estimation algorithm uses the random nature of the received signal from the communications between base stations (BS) and (UE) to calculate the estimated (AOA) without needing extra communication overhead(extra messages), and the computation process will be offline [6].

More specifically, source (BS) and target (BS) will use the estimation algorithm in section (2.2) to calculate the estimated (AoA).

Revised Manuscript Received on February 28, 2020.
* Correspondence Author

Mohamed S. Abdelhady*, Department of Communication Engineering, Ain Shams University, Cairo, Egypt

Wagdy R. Anis, Department of Electrical Engineering, Ain Shams University, Cairo, Egypt

Ahmed A. Abdel-Hafez, Department of Communication Engineering, Military Technical Collage, Cairo, Egypt

Haitham D. Eldemerdash, Department of Communication Engineering, Military Technical Collage, Cairo, Egypt

Amr Abdelaziz, Department of Communication Engineering, Military Technical Collage, Cairo, Egypt

Estimated (AOA) is a truly random value which will be used as a key seed and then this seed will be used with cryptographical tools such as universal hash functions to generate a truly random secret key (256 bit) after modifying the value of (AoA).

Secret key will be used as Transmission Encryption Key (TEK) in phase 1. Then the estimated (AoA) at the target (BS) will be compared with the expected range Θ_{EXP}: (Θ_0 to Θ_1),

where the legitimate (UE) is expected to connect to target (BS) in phase 2.

We assume that the cell is hexagon with six edges and conducted with each adjacent cell through certain edge, each edge occupies certain range = 2π/6, (Θ_0 to Θ_1). So, our frame work provides two phases of exhausted work against any attacker who claims to be a legitimate user (impersonation attack) and to the one who try to attack as man in the middle to spoof communication messages or to disclose TEK.

In case of the attacker passed through the first phase, and it is theoretically impossible with the existing computations capabilities to disclose and to find the key with length 256 bits even with using quantum computer the security strength of the key will be halved but still the truly random key with length 128 bits strong. Second phase reduce the range to attack the BS from 2π to be (2π/6).

Although there are many physical layer parameters like Received Signal Strength (RSS) [7], Channel State Information (CSI) [8], Angle of Arrival (AoA) [3, 4, 6], we choose (AOA) because it is a parameter with a contextual meaning, and can contribute in handover authentication decision. The proposed protocol comes as a solution for handover authentication problem in 5G mobile networks due to the potential frequent handovers and authentications processes in small cells architecture under the next attacks situations:

1. Attacker with stolen identity that intentionally try to connect to a target BS as a legitimate user (impersonation attack).

2. Attacker who spoofs communication messages between UE and BS in the network trying to obtain any useful information (man in the middle attack).

Related Work:

There is an extensive research done in handover authentication in 5G mobile network, readers may refer to [9] where the authors introduce Software-Defined Networking (SDN) into 5G as a platform to enable efficient and secure handover and privacy protection, their objective is to obtain seamless and secure handover with global management of 5G HetNets through sharing of user's security context information (SCI) between related access points. This (SCI) consists of some of physical layer attributes like (CSI) and (RSS).

Also, in[10] the authors propose a (SDN) - enabled fast cross-authentication scheme which combines cryptographic and non-cryptographic techniques and address the challenges of latency and weak security.

In[11] the authors give a summary of various non-cryptographic techniques for user authentication and device identification in wireless networks using physical layer parameters.

In[12] the authors use channel characteristics like virtual Angle of Arrival(AoA) and Angle of Departure(AoD), to generate the shared secret key between two devices.

In[13] the authors present the used method to generate the secret key from the estimated parameters, exploited its randomness and presented the metrics used to test the strength of the key.

II. SYSTEM MODEL AND PROPOSED PROTOCOL

A. System Model

As shown in Figure1, there is a mobile network consists of source BS, target BS, legitimate user (UE), an attacker, and the Mobility Management Entity (MME) which plays a significant role in handover procedures. We suppose that all nodes in the network (BS, UE) equipped with multiple antenna transceivers each antenna transceiver has an array size n > 1, yet, in case of a different array size at each node, it will not change the results. Similarly, we suppose to use a Uniform Linear Array (ULA) antenna configuration and, the same results can be obtained directly from any other antenna configuration by setting the proper array response vector [14].

The UE/BS messages will be divided into np packets, each packet will be sent over the air using the standard that will be used in 5G mobile network, in the form of ns (OFDM) orthogonal frequency-division-multiplexing symbols, over each subcarrier, we suppose that the channel to be flat, i.e., the used bandwidth is larger than the bandwidth of each sub channel. The discrete baseband equivalent channel (after fast Fourier transform (FFT) operation in the receiver node).

The received signal can be written as in (1).

$$Y[i,j,k] = H[i,j,k]X[i,j,k] + N[i,j,k] \qquad (1)$$

Where 1 ≤ j ≤ ns, 1 ≤ I ≤ np, and 1 ≤ k ≤ nsc, stand for the symbol index, packet number and subcarrier index respectively, X[i,j,k] ∈ Cn×1 is the transmitted signal restricted by an instantaneous maximum power. E[tr(X[i,j,k] X†[i,j,k])] ≤ P Also, H[i,j,k] ∈ Cn×n is the channel coefficients matrix between transmitting node and receiving target node. lastly, N[i,j,k] ∈ C $^{(n\times1)}$ is an independent zero mean circular symmetric complex random vector [6].

5G networks are designed to provide wireless access in a direct communication, line of sight (LOS) environment, consequently, we represent the channel as a Rician fading channel.

In the Rician fading model, the received signal can be divided into two components; one of them is the specular component that comes from the (LOS) path and the other is the diffused component due to ground reflections, scatters from neighboring buildings, obstacles, other objects in the environment or the non-line of sight component (NLOS). The LOS component can be deemed stable, however the NLOS component can be represented as a Rayleigh fading channel as in (2).

$$H = H^{nlos} + H^{los} \qquad (2)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Where $H^{nlos}$and H^{los} represents the NLOS and LOS components respectively in (3, 4) and where k is the Rician factor,$\Psi = s_r(\theta)s_t^{\dagger}(\phi), s_t(\phi)$ and $s_r(\theta)$ are the antenna array response vectors at the transmitter

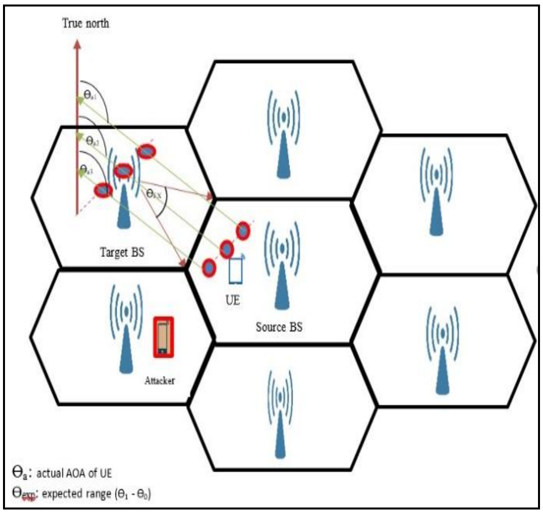


Fig. 1. System Model

and receiver respectively, θ and ϕ are the AoA and AoD of the transmitted signal respectively. $\widehat{H} \sim \mathcal{CN}(0, I_{n \times n})$ Represents the channel coefficients matrix for the NLOS signal component. We specify the contribution of the NLOS and LOS components to the signal with $\mu = \sqrt{k/(1+k)}$, $\sigma = \sqrt{1/(1+k)}$,as in (3,4) [6].

$$H^{nlos} = \sqrt{\frac{k}{1+k}}\Psi \qquad (3)$$

$$H^{los} = \sqrt{\frac{1}{1+k}}\widehat{H} \qquad (4)$$

B. AOA Estimation

Multiple signal classification (MUSIC) algorithm [15, 16] used to estimate (AOA) in our proposed protocol, it depends on the principle of orthogonality between the array response vector and the noise subspace Un. The main process in this algorithm is the Eigen value decomposition to the covariance matrix of the received signal. The generated covariance matrix is diagonal in nature.

From (1), we define $\boldsymbol{Q} = \boldsymbol{E}\,[\boldsymbol{YY}^{\dagger}]$ as the estimated observation covariance matrix which can be decomposed as in (5).

$$\mathrm{Q} = \mathrm{U}\,\Sigma\,\mathrm{U}^{\dagger} \qquad (5)$$

Where U and Σ are the matrices of eigenvectors and eigenvalues respectively. Note that U can be partitioned as U = [Us Un] where U_n and Us are the noise subspace and signal subspace, respectively.

Note that since the eigenvectors making up the noise subspaces unitary matrix (U_n) orthogonal to the signal steering vector(s), $s_r\ (\theta) \perp U_n$. The denominator turns into zero when (Θ) is equal to the signal direction. Thus, the estimated signal direction is the largest peak in the pseudo-spectrum, $P_{MUSIC(\Theta)}$ as in (6).

$$P_{MUSIC(\theta)} = \frac{1}{\sum_{m=1}^{M-D}\left|s_r^{\dagger}(\theta)U_n\right|^2} = \frac{1}{s_r^{\dagger}(\theta)U_nU_n^{\dagger}s_r(\theta)} = \frac{1}{\left\|U_n^{\dagger}s_r(\theta)\right\|^2} \qquad (6)$$

It worth to highlight that our estimation algorithm (MUSIC) doesn’t assume any specific signal structure, rather it exploits the random nature of the received signal, this in fact renders our (AOA) estimation algorithm independent on the underlying signal specific standard. And also we need to highlight that the idea of failure of MUSIC algorithm in mmwave channel due to rank defective which happens because of the coherent signals nature in mmwave channel is not an applicable case in our network, where we target single user at a time, but in case of ‘n’ users there is a modulation waveform used in the network which is orthogonal frequency-division multiplexing (OFDM) and this modulation enable the system to differentiate between different user, so the case of rank defective does not exist.

C. Proposed Protocol

As shown in Figure 2, we assume that UE is a legitimate user connected to a source BS and according to moving near the edge of his cell and measuring power strength levels from neighbours BSs. he needs to make a handover to another BS to keep his connection with the network with a certain level of quality of service (QOS). So, we introduce this protocol for fast and secure handover authentication in 5G mobile network **with following steps:**

Step 1: UE will collect power measurements from neighbours BSs and send them to source BS.

Step 2: Source BS will estimate AOA to the UE from the received signals without needing extra overhead communication. And then sends measurements and estimated AOA to MME to decide which target BS, the UE will connect with.

Step 3: MME will choose target BS and sends a UE information and estimated AOA to it, to use it as a seed to generate TEK. Also, MME will send the information about target BS to source BS, and generates the TEK.

Step 4: Source BS will send estimated AOA, target BS information to UE. Then UE will use the estimated AOA to generate TEK.

Step 5: UE will send an encrypted handover request with TEK to target BS.

Step 6: Target BS will use its generated TEK to decrypt handover request if it is ok it will estimate the AOA from the received signals to the UE and then will compare this AOA withθ_{exp}, which is the range where UE supposed to connect from it. If it is within dedicated range, it will accept the UE handover request and then send path switch request to MME encrypted with TEK.

Step 7: MME will send path switch acknowledgment (ACK1) encrypted with TEK to the target BS.

Step 8: Target BS will send handover confirmation acknowledgment (ACK2) to UE.

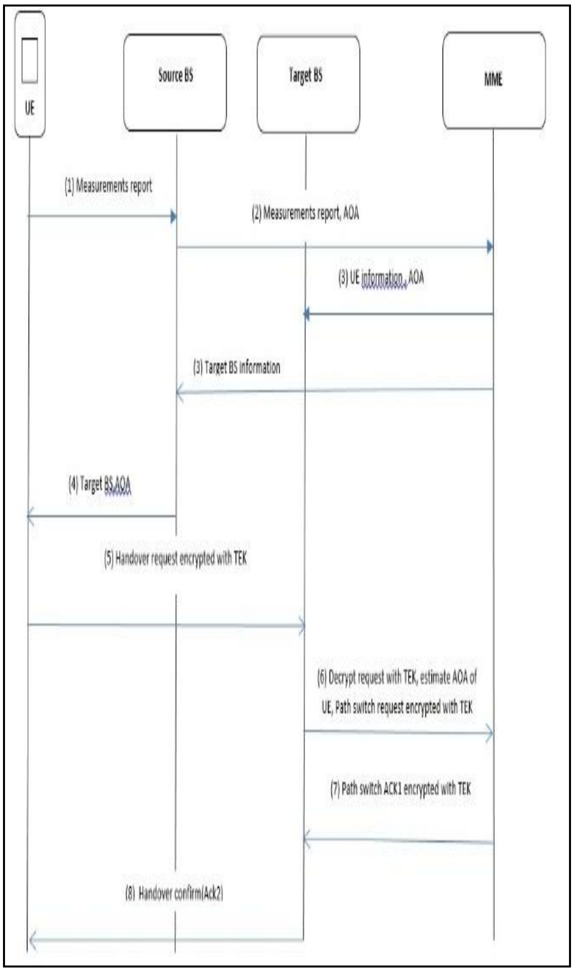

UE
Source BS
Target BS
MME
(1) Measurements report
(2) Measurements report, AOA
(3) UE information , AOA
(3) Target BS information
(4) Target BS,AOA
(5) Handover request encrypted with TEK
(6) Decrypt request with TEK, estimate AOA of UE, Path switch request encrypted with TEK
(7) Path switch ACK1 encrypted with TEK
(8) Handover confirm(Ack2)

Fig. 2. Proposed Protocol

III. RESULT AND DISCUSSION OF ATTACK MODEL AND SECURITY ASSESMENT OF THE PROPOSED PROTOCOL

A. Attack Model

As described before, we study an attacker with stolen identity that intentionally try to connect to a target BS as a legitimate user (impersonation attack).

And attacker who trying to disclosure the (TEK) and use it to claim that he is a legitimate UE or try to spoof communication messages between UE and BS (MITM).

Noting that in the considered attacks scenarios, messages received at the target BS will pass the system authentication framework, where It is recommended that the 5G authentication framework to be Extensible Authentication Protocol (EAP) and Key Agreement (EAP-AKA) [17].

B. Security Assessment of the proposed Protocol

We will use two tools to verify the security of the proposed protocol through **two phases**:

- **Phase(1) Security Assessment to the Proposed Protocol against MITM Attack Using AVISPA:**

AVISPA tool designed to Characterization cryptographic protocols and analyzing their security properties by looking for attacks for specified scenarios.

- **Proposed Protocol Description in AVISPA Tool:**

Proposed protocol description using the common algebraic language CAS, the protocol is described in 6 fields; the identifiers, the protocol message flow, the rules' knowledge, the session instances, the intruder possible knowledge, and finally the security goals we need to prove using AVISPA tool.

The CAS description of the proposed protocol is translated into HLPSL language using the SPAN tool. The HLPSL description is used as an input to the AVISPA animator SPAN for verifying the protocol design.

- **Proposed Protocol Security Verification:**

For proposed protocol security verification, we introduce a model where the intruder initial knowledge will be {user equipment (UE), source base station (SBS), target base station (TBS), mobility management entity (MME), key used by (MME) (KMME), measured power strength levels from neighbors BSs (Measurements), angle of arrival 1 (AoA1), angle of arrival 2 (AoA2), handover request (hreq),Path switch request (psr), path switch acknowledgment (ack1), handover confirmation acknowledgment (ack2)} also, the intruder can intercept and steal the messages between the communicated entities. As a result, we treat with an intruder pass the system authentication framework (EAP-AKA) and his messages to (MME) or source BS or target BS as they are originated from legitimate UE.

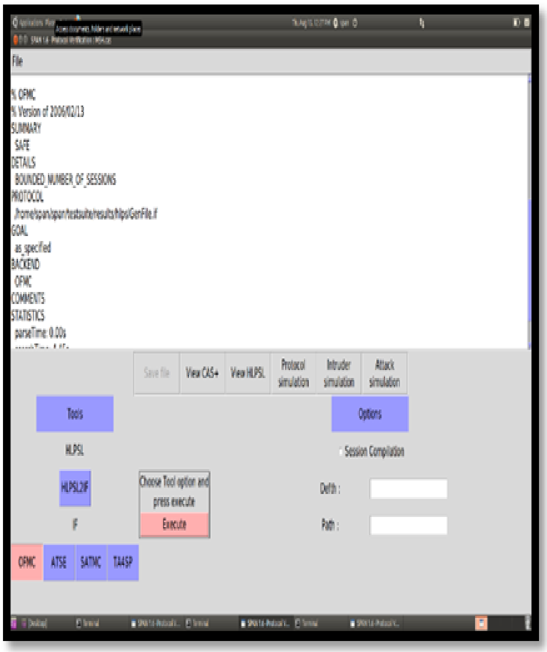
AVISPA tool with On-The-Fly Model-Checker (OFMC) model checker, performs protocol falsification and bounded verification. Constraint-Logic-Based Attack Searcher (CL-ATSE) will be used to prove the assigned security goals of the proposed protocol against MITM attack.

The protocol has a complete run and the (AoA) parameter is derived in the source BS side and distributed to MME then MME distributed it to the target BS side. Then MME, UE, target BS generate TEK which used in encrypting and decrypting handover request, ACK2 between UE and target BS, ACK1 and path switch request between target BS and MME. Also, there is no attack simulation, because the protocol is SAFE, and the AVISPA could not launch a trace for any attack.

The intruder in this model has tried to apply Man-In-The-Middle Attack (MITM) between the protocol entities, an intruder may intercept and steal all the transmitted messages and then may forward these messages, impersonating the legitimate user, trying to learn the TEK.

In spite of, the protocol with MITM attack has a complete run; the intruder could not add the TEK to his knowledge, where all the added knowledge is encrypted.

By executing the OFMC, CL-ATSE tools, protocol simulation, intruder simulation, attack simulation. we proved that; the protocol is safe (an intruder could not attack the protocol), and the specified security goals (secrecy of the TEK and the mutual authentication between the UE and the target BS) are verified where the attacker could not disclose TEK and add it to his gained information, as illustrated in Figure. (3,4).



```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/hlpsGenFile.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
 parseTime: 0.00s
```

Fig. 3. Security verification of the protocol

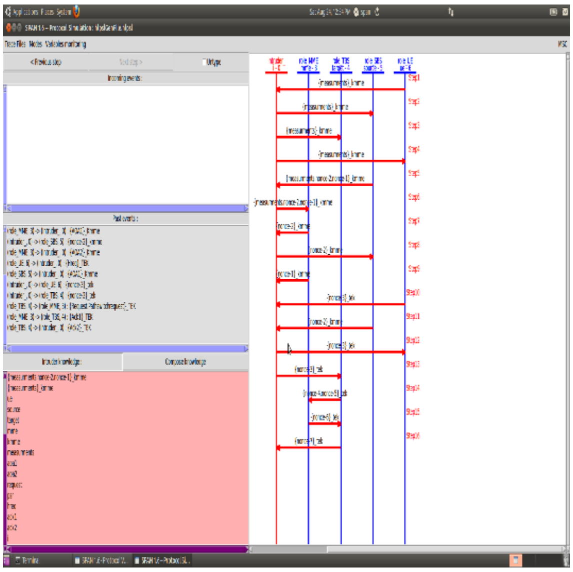


Fig. 4. Attacker's gained information

- . **Phase (2) Security Assessment to the Proposed Protocol against Impersonation Attack Using MATLAB:**

MATLAB used to verify that our protocol is secure against impersonation attack. The simulation results presented in this section depend on the following simulation setup.

We suppose that all communication nodes are equipped with multiple antenna transceivers, each of array size n =8. Yet, in case of a different array size at each node, it will not change the results.

Similarly, we use a Uniform Linear Array (ULA) antenna configuration and, the same results can be obtained directly from any other antenna configuration with straightforward manipulation. Payload messages are produced from a unit variance complex Gaussian random variable, zero mean, and scaled to satisfy the power constraint. We assume expected range, Θ_{exp} from 20° to 80°.

We evaluate phase (2) in terms of (PD) and (PF) where PD is a probability of detection and PF is a probability of false alarm.

PD is the ability of the system to take the right decision and accept the handover request after estimating (AOA) and compare it with the expected range θ_{exp} with different values of signal to noise ratio, (SNR).

PF is the probability that the system will fail in taking the right decision when comparing between the estimated (AOA) , expected range θ_{exp} and accept or reject handover request from a legitimate user or an attacker, due to miss calculating to the estimated (AOA).

PD and PF are functions of signal to noise ratio, SNR, for each SNR value we will estimate AOA for 1000 times then calculate both PD and PF, where they are the probability of the right and wrong decisions when the estimated (AOA) compared with the expected range, we will give two different scenarios:

1. We evaluate PD when a legitimate user located at (20°) at the boundary of the expected range.

   As shown in Figure 5, PD approaches 1 as SNR increase meanwhile, the same result holds true if an attacker located at 80°.

2. We evaluate PF, first we will consider an attacker located at 19.5° while he claims that he is in the Θ_{exp} from 20° to 80°.

   As shown in Figure 6. PF approaches 0 when SNR increases, and also the same result will be obtained if an attacker located at 81°.

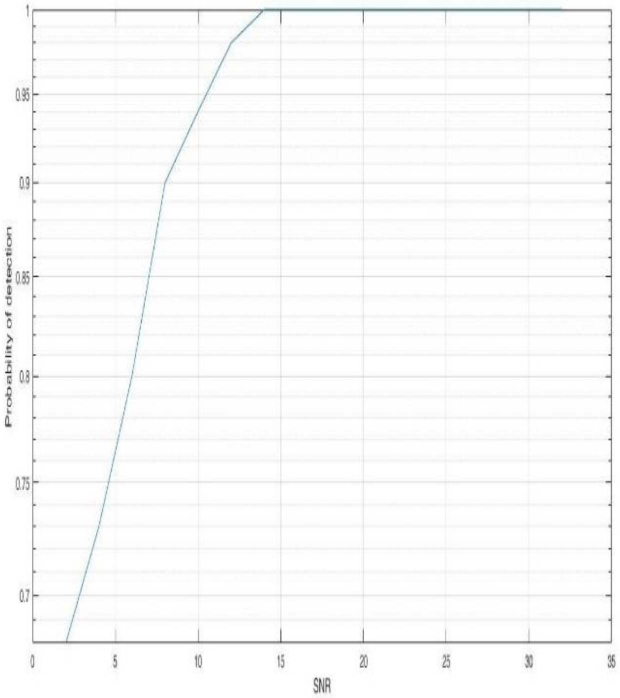


Fig. 5. PD as a function of SNR for UE located at the boundaries of Θ_{exp}

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

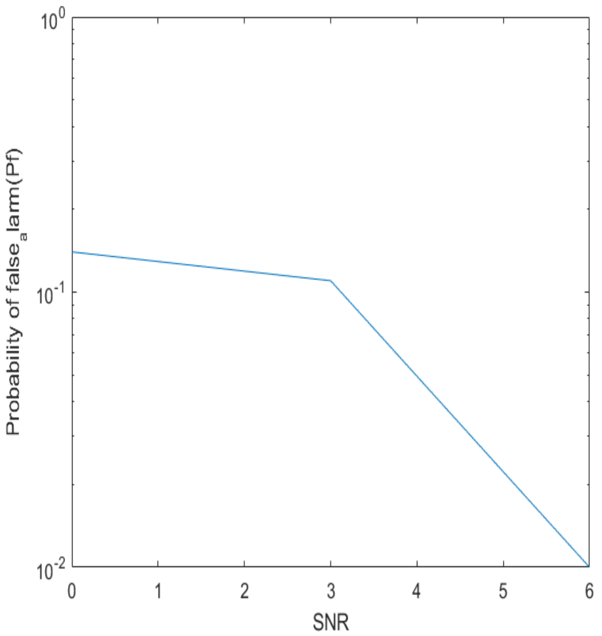


Fig. 6. PF as a function of SNR for an attacker located at 19.5◦

IV. CONCLUSION

This paper provides a detailed description of the proposed handover authentication protocol for 5G mobile network where we use a physical layer attributes (AoA) as seed to generate a truly random key used as a TEK and merged between cryptography and non-cryptography techniques in our protocol, the provided security gain comes with no extra communication overhead, bandwidth as opposed to security solutions provided in the upper layers. The security verification for proposed protocol is achieved by using AVISPA and MATLAB..

REFERENCES

1. N. Panwar, S. Sharma, and A. K. Singh, "A survey on 5G: The next generation of mobile communication," Physical Communication, vol. 18, pp. 64-84, 2016.
2. M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," IEEE Communications Surveys & Tutorials, vol. 18, pp. 1617-1655, 2016.
3. T. E. Tuncer and B. Friedlander, Classical and modern direction-of-arrival estimation: Academic Press, 2009.
4. Z. Chen, G. Gokeda, and Y. Yu, Introduction to Direction-of-arrival Estimation: Artech House, 2010.
5. J. Xiong and K. Jamieson, "Securearray: Improving wifi security with fine-grained physical-layer information," in Proceedings of the 19th annual international conference on Mobile computing & networking, 2013, pp. 441-452.
6. A. Abdelaziz, R. Burton, F. Barickman, J. Martin, J. Weston, and C. E. Koksal, "Enhanced Authentication Based on Angle of Signal Arrivals," IEEE Transactions on Vehicular Technology, vol. 68, pp. 4602-4614, 2019.
7. A. Kitaura, H. Iwai, and H. Sasaoka, "A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio," in The 9th International Conference on Advanced Communication Technology, 2007, pp. 1763-1767.
8. X. Sun, W. Xu, M. Jiang, and C. Zhao, "Improved generation efficiency for key extracting from wireless channels," in 2011 IEEE International Conference on Communications (ICC), 2011, pp. 1-6.
9. X. Duan and X. Wang, "Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer," in 2016 IEEE International Conference on Communications (ICC), 2016, pp. 1-6.
10. 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), 2018, pp. 1-7.
11. M. R. Kanjee and H. Liu, "A generic authentication protocol for wireless body area networks," in Proceedings of the 8th International Conference on Body Area Networks, 2013, pp. 502-508.
12. L. Jiao, J. Tang, and K. Zeng, "Physical Layer Key Generation Using Virtual AoA and AoD of mmWave Massive MIMO Channel," in 2018 IEEE Conference on Communications and Network Security (CNS), 2018, pp. 1-9.
13. A. Badawy, T. Elfouly, T. Khattab, A. Mohamed, and M. Guizani, "Unleashing the secure potential of the wireless physical layer: Secret key generation methods," Physical Communication, vol. 19, pp. 1-10, 2016.
14. P. Gupta and S. Kar, "MUSIC and improved MUSIC algorithm to estimate direction of arrival," in 2015 International Conference on Communications and Signal Processing (ICCSP), 2015, pp. 0757-0761.
15. R. Schmidt, "Multiple emitter location and signal parameter estimation," IEEE transactions on antennas and propagation, vol. 34, pp. 276-280, 1986.
16. P. Stoica and A. Nehorai, "MUSIC, maximum likelihood, and Cramer-Rao bound," IEEE Transactions on Acoustics, speech, and signal processing, vol. 37, pp. 720-741, 1989.
17. E. U. T. R. A. Network, "3rd generation partnership project; technical specification group services and system aspects; general packet radio service (GPRS) enhancements for evolved universal terrestrial radio access network (E-UTRAN) access," EUTRA Network, 2011.

AUTHORS PROFILE

M. Said Abdelhady He received his B.Sc. from the Communication Engineering Department, Military Technical College, Cairo, Egypt in 2005, master student in Ain shams university communication and electronics Department. Currently, member of cryptography research center since 2014, Egyptian Armed Forces.

Wagdy R. Anis He received his B.Sc. from the Electrical Engineering Department, Ain shams university, Cairo, Egypt. M.Sc. from Ain shams university in 1977. Ph.D. in 1985 Currently Emeritus Professor at Electronics Engineering and Electrical Communications.

Ahmed A. Abdel-Hafez He received his B.Sc. and M.Sc. from the Communication Engineering Department, Military Technical College, Cairo, Egypt in 1990., 1997 respectively. Ph.D. from Ottawa University in 2003. Currently Head of cryptography research center since 2012, Egyptian Armed Forces. His research interests including Applied cryptograph, and Information Security.

Haitham D. Eldemerdash He received his B.Sc. and Ph.D. from the Communication Engineering Department, Military Technical College, Cairo, Egypt in 2002, 2014 respectively. and the M.Sc. from Arab academy for science and technology, Cairo, in 2011. Currently, member of cryptography research center since 2014, Egyptian Armed Forces.

Amr Abdelaziz, received the B.Sc. and M.Sc. degrees in 2005 and 2012 from The Military Technical College, Cairo, Egypt, and the Ph.D. degree from The Ohio State University, Columbus, OH, USA, in 2017. He was a Senior Naval Communication Officer from 2005 to 2007, a Teaching Associate with the Military Technical College from 2007 to 2014, and a Graduate Research Associate with The Ohio State University from 2014 to 2017. He is currently a faculty member with The Military Technical College.

.