TPA: Prediction of Spoofing Attack using Thermal Pattern Analysis in Ultra Dense Network for high speed handover scenario

Garima Chopra¹, Student Member, IEEE, Rakesh Kumar Jha¹, Senior Member, IEEE and Sanjeev Jain², Member, IEEE

¹Electronics and Communication Department, Shri Mata Vaishno Devi University, Katra, J&K, India
²Computer Science Engineering Department, Shri Mata Vaishno Devi University, Katra, J&K, India

Corresponding author: Rakesh Kumar Jha (e-mail: jharakesh.45@gmail.com).

This work is supported by 5G and IoT Lab, Department of Electronics and Communication Engineering, and TBIC-Shri Mata Vaishno Devi University, Katra, Jammu (India).

ABSTRACT With the rising demand for high data rate by the subscribers, security becomes a prominent and critical issue for the emerging Ultra Dense Networks (UDN). Although, more Access Points (AP’s) are involved with the purpose to strengthen the signal quality and aid in User Equipment (UE’s) throughput enhancement. Thus, UDN serves as a promising approach to accommodate a large number of AP’s (and UE’s) and ensure them with seamless connectivity and ubiquitous coverage. However, this intensification of Base Station (BS) densities will upsurge the handover (HO) rates for high-speed users. In this context, this paper investigates the security issues for the roaming users in UDN, pertaining to increased handover percentage. Towards this goal, a novel approach called as Thermal Pattern Analysis (TPA) is proposed to determine the probable region of attack, for high-speed users through tracking their footprints of thermal energy patterns (i.e. Energy and Spectral Efficiency). We also perform the Secrecy Capacity check on wandering users, considering the fact that eavesdropper (or Eve) location is erratic. Comprehensive simulations are performed for real-time deployment and results validate the effectiveness of the proposed approach. Consequently, thermal analysis can be performed for all variety of mobile communication scenarios to uncover the adversary tremor. A real-time implementation using hardware components related to the prototype study has been carried out to access the performance in the actual world. From the analysis of the results, it is quite evident that TPA is more accurate in finding the probable region of low security for the UDN environment.

INDEX TERMS UDN, Energy Efficiency (EE), Handover, mobility, TPA, Secrecy Capacity, and Spectral Efficiency (SE).

I. INTRODUCTION

Due to explosive proliferation of mobile user equipment (UE), densification of the wireless network is proposed as an alternative approach to catering to the 1000x folds demand of network capacity and high Quality-of-service (QoS) [8], [10], [28]. Undoubtedly, 5G technology is commissioned with ultra-dense (UDN) environment provisioned with high small cell BS density and supporting high rate multimedia applications [4]. Conceptually, UDN can be categorized as a type of network with little inter-site separation between the devices and the APs, capable of generating low-interferences level while transmission, with the purpose to fulfill high data rate requirement of the present era [29]-[30]. Another definition of UDN considers it to be a collection of heterogeneous networks from sensors, mobiles, to wearable devices, etc. [9]. Thus, security has to turn out to be a prime objective which requires the widespread attention of the researchers. Nowadays, physical layer security (PLS) is given full-attention in order to curb the arising security challenges by the next generation of wireless communication. Also, the PLS techniques prove to be a complement against traditional encryption techniques which puts an irrelevant computational burden on low power devices [34]-[35].
Apart from this, UDN also guarantees to support the connection to high speed (or moving) users, up to a speed of 500 Km/hr. All these benefits come at a cost, as the moving users (low or high mobility) tend to experience the sudden rise in the handover rate, due to the installation of low-power and low-coverage APs (or Base Stations, BSs) [16], [17]. Thus, the confidentiality and integrity of moving users are at stake with the rise in handover rates [5] and overheads as a result of close proximity between the users and small cell BSs [40]. Moreover, the existing policies for the protection of moving users cannot be directly applicable to the UDN. Thus, proper polishing and redesigning of the existing schemes and algorithms ought to be performed, for protection of UE’s in UDN. To the best of our knowledge, the handover related security issues is an open challenge and the most frequently occurring event at present, for secure UDNs.

A. BACKGROUND OF RESEARCH AND RELATED WORK

In our previous work [17], we proposed the methodology for extracting the handover zone in case of UDN, for high-speed users. However, the approach is based on the Signal to noise ratio (SNR) variation and Channel Quality Indicator (CQI). This has also taken into account the fading conditions and also how the speed variation will impact the pattern of SNR’s for a targeted user(s). Based on the previous work, we advance our work in this paper by proposing a method for detection of the probable zone of attack on the basis of energy (or thermal) pattern analysis for speedy users. The picocells have purposely opted here for the considered case study in previous and current work, the reason for this is that picocells are low power and low coverage cells. Their sole purpose is to enhance the capacity. They are featured with all the basic competence of macrocell and can act as a substitute for macrocell. The previous work also included the basic architecture of UDN along with the problem which has been highlighted here, which we have comprised in our work. Along with this, we also proposed the security architecture for UDN, typically arranged in order of their risk factors in [13].

To ensure secure handoff’s, we need to protect the moving UE’s connected to low power BS so as to facilitate the UE to seamlessly attach with neighbouring AP. Recently in [18], the authors investigated the impact on the capacity of UE with the increase in density of eavesdroppers and concluded that positive secrecy capacity can still be achieved in UDN. Consequently, the secrecy capacity is examined for heterogeneous networks in [19], without keeping the track for BS and UE densities. Similarly, secrecy outage probability (SOP) is checked for Multi-RAT scenario in [20] and for dense conditions, the authors in [21] approximated the closed form expression for SOP. None of the work considers the energy dissipation as the weapon for tracing the user’s attacked location.

As explained earlier, the deployment of UDN brings about an impressive improvement in services to end users. But, it also brings about the new possibilities of security loophole. The pictorial representation of UDN security challenges is shown in Fig 1. However, the study related to security in UDN is still in the initial phase of implementation and an immature field. Several issues have been put forward while UDN is considered and few major issues have been listed as follows [12]-[13], [34]:

i.) The introduction of a large number of small cells provide a new platform for substantially high data rate support. Eventually, contributing towards the high interference from the adjoining cells which can be further reduced by employing proper mitigation strategies. Additionally, the security of the users sharing a common region with one or more adjacent small BS(s) is also an important aspect which requires proper attention, as the transmission can be affected by the jamming signals from the attacker with a simultaneous rise in computational complexity. But using closed access groups and by prioritizing the user’s traffic based on their application demand will provide as an alternative, to serve as a balance between security and complexity.

ii.) The introduction of intermediate nodes like jammers will put an unnecessary burden on the network performance of the UDN. This will put forward an idea for new existing heterogeneous nodes for secure design. Also, in literature, it has been mentioned that relays can serve as dedicated and friendly jammers. This would also benefit in the maintenance and installation of jammers. In a UDN scenario, the use of multiple jammers is stressed in order to provide reliable and interminable services.

iii.) The users are expected to surpass many small cells within a fraction of seconds. Hence, the security is also a prominent issue in the network, when moving users are stressed on. Due to the availability of large small BS density, the choice of the appropriate legitimate BS is also a challenging task in its own way.

iv.) The user’s ability to deploy self-made BSs for personal use will originate many research and security challenges. Also, the user should be able to differentiate between the malicious BS and the real one. Along with this, resource allocation and network configuration for different users also bring additional challenges. Since it is highly desirable to
maximize the secrecy performance of UDN along with innovative resource management technique.

In addition, the limited bandwidth and broadcast nature of the communication medium left in a difficult situation, where security features like authenticity, confidentiality cannot be provisioned to each device. These aspects cannot be satisfied with the long-established approach of encryption. However, new security paradigms need to be defined, to adhere to the advanced features enabled in UDN like low latency, EE etc. [22].

The nodes, which are limited in computational capabilities [23], a fusion centre is created for protection from jamming attack in the 5G scenario. In [24], frequency hopping is used in SDN as a solution for jamming in 5G against DoS (Denial of Service). EE can be improved by normally controlling the power consumed by the nodes, and due to the high availability of small BSs under a macrocell for UDN, power consumption is also a big issue which needs to be taken care in correlation to security. The PLS and EE for Massive MIMO are extensively studied in [25], in Het-Net.

Most of the existing works on the security of 5G consider a single antenna deployed at small cells BS. Assuming that the eavesdropper and relay equipped with single antennas [26], the secure transmission is designed in 5G. The results reveal that when the relay is featured with multiple antennas, SOP considerably improves for the destination node. AN (artificial noise) can be served as an optimum choice. There are two important parameters defined in literature to evaluate the performance of the security algorithms, namely Secrecy capacity and SOP. For proper estimation of the network performance, the stress on minimizing the SOP and aspired value of secrecy capacity is given for physical layer protection. AN secure transmission is proposed in [27] where the sender is loaded with multiple antennas for millimetre-wave (mm-wave) transmission with partial knowledge about CSI of Eavesdropper [14].

Recently, in [37], the authors executed the physical layer message authentication by comparing the channel estimates with the predefined estimation of the signal. Additionally, they derived the attacking strategy and obtained the tightest bound on error region. Similarly, the message authentication via fingerprint scanning projected in [38] rather than relying on the channel characteristics. The authors in [39] proposed the RSSI (Received Signal Strength Indicator) based authentication scheme along with FW (Frank-Wolfe) algorithm to detect the spoofing attack in the multiple landmarks, thus reducing the computational overheads and achieving higher accuracy. All the recently stated works focused on the authentication scheme either by partially or fully assuming the CSI of Eve, nevertheless the proposed approach only considers the estimation about the energy requirement, rather it depends purely on the CSI of the legitimate users. However, none of the aforementioned works examine the effect of an eavesdropper on the performance of moving users.

B. RESEARCH CONTRIBUTIONS

The main contribution of this paper is that we propose a novel scheme for detection of a probable region of attack by the eavesdropper for UDN, whilst by the energy consumption of the moving UE. The key contributions of the paper are listed as follows:

- Taking the handover related security concerns for moving UE’s in UDN, we design an approach through which accurate position of the attack can be estimated through matching of minimum energy requirement in the area with the actual value of energy consumption observed in the Region of Interest (RoI).
- In this paper, we also perform the secrecy capacity analysis for mobile (moving) UE’s, by considering various channel losses (like time-varying nature, path loss, shadowing loss etc.). The results are evaluated for both the active and passive nature of the eavesdropper.
- The results in [17] are compared with the methodology adopted in this paper. The results reveal that this energy-based approach (TPA) is more versatile and accurate in comparison to [17].
- We also derive the closed-form expression for secrecy capacity for mobile UE’s, considering various features of UDN.
- In extension to above-mentioned contributions, we also perform the prototype study for real-time testbed analysis of TPA, to analyse the behaviour of the model in the actual conditions.

The flow for rest of the paper is as follows: Section II comprises the system model based on mathematical equations derived especially for our model, section III represents the problem formulation and discusses the proposal in detail, section IV discusses the proposed approach (TPA) in detail, section V consists of results and discussions in detail and section VI describes the conclusions derived by the simulation as well as experimental work.

II. SYSTEM MODEL

In this section, we present the adopted system model along with wireless channel model description, followed by a problem description.

A. DESCRIPTION

We consider a downlink transmission in UDN consisting of $k$ picocell BSs, with a maximum transmission power $P_{tx}$ serving up to $R$ meters and $N$ UE’s in the presence of $E$ eavesdroppers, all of them are distributed according to homogenous Poisson Point Process (PPP). Out of $N$ UE’s, some users are stationary and some are moving with a speed $v$. The eavesdropper nature may be active or passive, whose sole purpose is to overhear the information of the UE’s (moving UE’s in our case). Assuming that eavesdropper’s channel state information (CSI) is unknown at the BS. We further assume that the density of BSs is expected to be either higher or equivalent to UE’s density and eavesdropper’s density is much lower in comparison to that of UEs ($E \ll N$). In order to reduce the inter-cell interference, the orthogonal
resource blocks (RBs) are employed to separate $k$ independent picocell BSs. In this way, each UE can be served by multiple BSs through mutual cooperation among them and this approach is termed as Multiple Association (MA). This approach is beneficial to moving or speedy users as MA will reduce the overheads generated due to frequent handovers in the UDN architecture and also improves QoS for a high-speed UE.

The diagrammatic presentation of Thermal Pattern Analysis (TPA) is depicted in Fig. 3, wherein both the circles show the picocell coverage BS namely BS$_1$ and BS$_2$ and (BS$_1$ & BS$_2$) $\in k$. For analysing TPA strategy, the user $u_i$ tends to change its position at every instant of time $t$, where $(X_1,Y_1)$ shows the position of $u_i$ at $t_1$ and so on.

Let $(X_p,Y_p)$ and $(X_{p-1},Y_{p-1})$ denote the current and preceding position, respectively and the comparison of the energy consumed $E_p$ by $u_i$ for $(X = X_p,Y = Y_p)$ is made with $E_{p-1}$ for $(X = X_{p-1},Y = Y_{p-1})$. This is the approach through which energy traces (patterns) are formulated, using the approach of TPA. Here, in TPA, after the comparison of the situation of UDN, with the densification of the network [32].

In this paper, we use the practical 3GPP two-piece Path Loss Model shown in [33], wherein the model rely on the Line-of-sight (LoS) and Non Line-of-sight (NLoS) probabilities. Then, the average path loss between the UE $i$ and BS $k$ has a dependency on the following functions and is given by

$$\delta_{i,k} = \begin{cases} \rho_L(d_{i,k}^p)^{-\alpha_L}, & \text{Pr}_L(d_{i,k}^p) ; \text{LoS Prob} \\ \rho_{NL}(d_{i,k}^p)^{-\alpha_{NL}}, & 1 - \text{Pr}_L(d_{i,k}^p) ; \text{NLoS Prob} \end{cases}$$

where $\rho_L$ and $\rho_{NL}$ denote the LoS and NLoS path losses for a reference distance, respectively. Furthermore, $\alpha_L$ and $\alpha_{NL}$ represent the LoS and NLoS path-loss exponents, respectively.

The LoS probability is divided into two segments, which is shown below:

$$\text{Pr}_L(d_{i,k}^p) = \begin{cases} 1 - 5e^{-\gamma_1/d_{i,k}^p}, & 0 < d_{i,k}^p < d', \\ 5e^{-\gamma_2/d_{i,k}^p}, & d_{i,k}^p > d', \end{cases}$$

where $\gamma_1, \gamma_2$ and $d'$ denote the shaping parameters, where continuity of $\text{Pr}_L(d_{i,k}^p)$ is assured.

In 5G and beyond, the signal transmission occurs between BS and devices at a frequency band of $6 \, \text{GHz}$. However, extensive testing and studies are being conducted until now in the literature, to precisely measure the channel losses from $6 \, \text{GHz} - 32 \, \text{GHz}$, for both indoor and outdoor environments [29]-[31]. All these studies have been performed for crowded and dense scenarios which procure UDN within the measured results. Due to the small proximity between users and serving BS, the channel condition of devices operating in the above mentioned frequency range differs unexpectedly. For a cell radius of 200 m, the attenuation loss from the atmospheric absorption as low as $0.1 \, \text{dB}$ in mm-wave band ($> 28 \, \text{GHz}$) for outdoor communication. It is already known that small-scale fading occurs either due to multi-path components or motion of user (or serving BS). Further, the discussion regarding the impact of Doppler spread on channel gain of the user is accomplished in Section

Figure 2. Proposed System Model (TPA) for security analysis in High Speed Handover scenario.
V. However, several tests have been conducted for the measurement of multi-path delay spread, by taking indoor and outdoor conditions. Such as in [28], the authors proved that by using horn antennas at the side of both transmitter and receiver, the RMS delay spread ($\tau_s$) for NLoS and LoS scenarios is below 1.5 ns and 3.1 ns. Overall, after performing the analysis for $\tau_s$ by taking different antennas, it has been concluded that the value of $\tau_s$ is always less than 6 ns [28]. It has been further analysed from literature that omnidirectional antenna is more suitable for time dispersive analysis rather than horn antenna, at the receiver side. The authors in [32]-[33] experimentally studied the 3D-Stochastic channel models, delays and RMS delay spread in New York City for urban LoS and NLoS environment, in mm-wave frequency band. Hence, the impact of the multi-path delay spread is dominant when $\tau_s$ is greater than the inverse of the bandwidth ($B^{-1}$) allocated to the user.

Consider a simple example that only one RB is assigned to a particular user, then the inverse of bandwidth $B^{-1} = 5.55 \mu s$ which is more than $\tau_s$ i.e. ($\tau_s < B^{-1}$). Hence, there is only one dominant component in the 5G transmitted signal for the users, which is LoS component. Also, the $\tau_s$ has a dependence on the number of scatters, $\lambda_s$. Assuming that $\tau_s$ be the RMS delay spread of one scatterer and $\lambda_s = \phi$(constant), then generalized equation for total RMS delay spread can be defined as $\tau_s = \phi \times \tau_s^{'}$ seconds.

Hence, there will be no Inter-symbol interference (ISI) between two adjacent bits of information. Further, the channel will fluctuate principally due to large scale fading. Additionally, in order to reduce the impact of ISI or $\tau_s$, the bandwidth of user and guard bands should be carefully designed especially for the moving users.

C. ADVERSARY MODEL

Consider a similar scenario as shown in Fig. 3, where eavesdroppers are randomly distributed within the coverage range of BS1. However, for moving UEs, the probability of success rate of attack purely depends on the exact and precise location of the UE under attack. The primary goal of the attacker is to determine the nature of the UE and its probable locations for the next few instances, for a given geographical area. In the next step, the adversary will try to disconnect the services to the UEs, and force them to connect with the less reliable and less secure network. In our case, the adversary model is categorized into three modes, as explained below:

1) Passive Mode: The adversary silently tries to sniff the information exchanged between UE and the BS, over the allocated channel. In this type of attack, the adversary sole purpose is to extract the useful information without impairing the signalling messages.

2) Active Mode: The adversary can set up its own Rogue AP in the communication region of UEs. This type of attack is more harmful in comparison to the passive adversary. Since an active adversary will deny the services of UE.

3) Opportunistic Mode: In this mode, Eve will behave in an intelligent manner. It will silently observe the movement and the traffic pattern of a user, under attack and will wait for the worst condition or the weakest state of the user to occur. Alternatively, this type of behaviour is a combination of active and passive nature.

Consequently, the received signal between the $k^{th}$ serving BS and eavesdropper $E$ is given by

$$\gamma_E = p_{tx,E} G_k^E \frac{e^{j\delta}}{\sigma_E^2},$$

where $I$ denotes the interference and $\sigma_E^2$ shows the variance of Additive White Gaussian Noise (AWGN) with zero mean, by $E$ through serving $k^{th}$ BS. Hence, the achievable rate by $E$ can be predicted by Shannon theorem as

$$C_E^k = B' \times \log_2(1 + \gamma_E) \text{bps},$$

$$\Rightarrow C_E^k = B' \times \log_2 \left(1 + \frac{p_{tx,E} G_k^E}{\sigma_E^2}\right).$$

Herein, we assume that $P_{tx,E}$ is very less as compared to $P_{tx}$ ($P_{tx,E} < P_{tx}$). In our condition, the adversary will behave in an opportunistic mode.

D. TRANSMISSION MODEL

In our model, the total transmit power $P_{tx}$ of the $k^{th}$ serving BS is distributed among $N$ UEs, which is denoted by $p_{tx,k}$. Accordingly, the signal received by user $u_i$ from serving BS $k$ at $p^{th}$ position in the presence of eavesdropper $E$, is given by

$$\gamma_{k,i} = \frac{p_{tx,k} G_{k,i}}{I_i + N_i}.$$

where $I_i = \sum_{j=1,j \neq BS}^{N} P_{tx,i} G_{i,j} + \sum_{j=1,j \neq BS}^{N} P_{tx,i} G_{j,i}$ is the aggregate of the interference power gathered by $u_i$ at $p$ and $N_i$ shows the AWGN with zero mean and $\sigma_i^2$ variance.

Accordingly, the achievable rate $C_{k,i}$ can be expressed as

$$C_{k,i} = \lambda_k \times B_i \times \log_2 \left(1 + \frac{p_{tx,k} G_{k,i}^2}{I_i + N_i}\right) \text{bps}, \lambda_i = 0 \text{ or } 1$$

(7)

From the expression of Shannon Capacity, it is beneficial to put the BS into sleep mode when the density of UEs drops below a certain limit or the BS is not serving for a quite long period of time. Thus, $\lambda_k$ depends on the mode of operation of BS either sleeping ($\lambda_k = 0$) or in awake state($\lambda_k = 1$).

Let us define secrecy capacity, $C_s$ which can be represented as the number of bits (in bps/Hz) that can be successfully transmitted from source (BS) to destination ($u_i$), without being intercepted by the eavesdropper ($E$) and given by [15]

$$S_c = \left[ C_{k,i}^p - C_E^k \right]^t.$$

(8)

For secure transmission in UDN, $S_c$ should be positive ($S_c > 0$) and greater than the required threshold ($S_c > S_{c,th}$). In case of UDN, non-zero secrecy capacity probability is very high typically greater than 0.95 [11] & [12] i.e.

$$Pr(S_c > 0) > 0.95,$$

(9)

Hence, for detection of attack in the region, the following conditions need to be satisfied and is given by

$$S_c = \begin{cases} S_c \geq 0, & \text{mandatory}, \\ S_c \geq S_{c,th} \pm \epsilon, & \text{no attack}, \\ S_c < S_{c,th} \pm \epsilon, & \text{attack}. \end{cases}$$

(10)

We define a parameter $\epsilon$ to show marginally the error in $S_c$ when we define the measurements and $\epsilon$ comprises of channel gain.
estimation error, CSI of eavesdropper which is unknown at the transmitting end, etc.

As described earlier, in this paper, we address EE of the moving user for tracing the pattern in terms of the amount of bits transmitted per joules energy consumption. EE can be defined as the ratio of total throughput (or capacity) to the total power consumed and can be given by

$$\eta_{EE} = \frac{c_{k,i}^{ref} + \sum_{j=1}^{n} c_{k,i}^{p}}{p_{t}^{ref} + \sum_{j=1}^{n} p_{t}^{p}}$$

where $\eta_{EE}$ is in bits per joule. Specifically, in UDN, the greater density of UE’s will lead to a lower value of EE as the power consumption rises and this will prima lead to degradation in the performance. Through this work, the main purpose is not to improve performance metrics but to observe the nature of the user. Similarly, SE can be defined as the number of bits transmitted per unit bandwidth (bps/Hz) and can be given by

$$SE = \frac{c_{k,i}^{ref} + \sum_{j=1}^{n} c_{k,i}^{p}}{p_{t}^{ref} + \sum_{j=1}^{n} p_{t}^{p}}$$

Since the transmit power of picocell BS is far less than macrocell BS then the QoS of a legitimate user is essentially influenced by the small variation in the channel coefficients. Hence, with the increase in velocity of user or distance between user-serving BS, the channel condition varies sharply.

E. POWER CONSUMPTION MODEL

In this strategy (TPA), we need to find out the highest point of energy dissipation, which depends on the channel parameters, the power transmitted by the BS and power consumed by the UE. As far as total power consumption by BS for a particular UE is concerned, it is a combination of power assigned by serving BS and the total static power. According to [1, 2], the power consumption of BS $k$ can be demonstrated as

$$P_k = \begin{cases} \frac{1}{\eta} p_{t}^{k,i} + n_u P_u, & \text{if } \lambda_k = 1, \\ n_u P_s, & \text{if } \lambda_k = 0, \end{cases}$$

where $P_u$ and $P_s$ denote the static power consumed per antenna during active and sleep mode, respectively. Whereas, $n_u$ shows the number of antenna elements on the serving BS (i.e. k).

Note: The power consumption during sleep mode is independent of bandwidth. It mainly depends upon the mode in which BS is sleeping [3].

Extraordinarily, the activation probability of a particular BS $k$ can be expressed as [41]

$$P_{ua} = 1 - \left[1 + \frac{1}{3.5 r} \right]^{-3.5},$$

where $r = \frac{\lambda_u}{\lambda_u}$ can be defined as the ratio of small cell BSs density (\(\lambda_u\)) and UEs density (\(\lambda_u\)).

F. ENERGY CONSUMPTION MODEL

We formulate a security problem during handover as TPA that allows us to accurately reflect the anomalous behavior of a device in the state of motion. In this TPA approach, our goal is to appropriately define the energy consumption of user either in motion or in the stationary state. So that we can trace the energy requirement of any given user, for a particular area, without disturbing the on-going transmission. However, the energy consumption of any device depends on the power allocated to device and total time for which the transmission occurs (including various delays). The energy consumption of any device or node is a function of energy required to transmit one bit of information ($E_p$), energy consumed by RF components ($E_{RF}$), extra overheads generated during handover decision and execution phases ($E_{HO}$) and can be expressed as

$$E_t = E_p + E_{HO} + E_{RF}$$  

$$E_{HO} = E_{user} + P_{user} \times P_{fail},$$

where $E_{user}$ denotes the energy required during the switching of network from serving to target BS. $E_{user}$ diverges according to the type of serving and target BS.

In order to complete the description about TPA, we need to provide the details of the remaining function that contributes towards the estimation of the threshold value of energy for any device/node. As mentioned earlier, the energy consumption of any device also depends on the transmission time and the delays. In wireless communication, there are many delays that a device will experience such as transmission delay, propagation delay ($T_p$), processing delay and handover delay. The transmission delay $d_t$ (in seconds) for any user $k$ can be expressed mathematically as

$$d_t^k = \frac{n_s}{n_b} + t^h,$$

where $n_s$ and $n_b$ denote the number of symbols and data rate from BS to user (in bps/Hz), respectively. $t^h$ represents the time span (in seconds) for handover information gathering and preparation. Unfortunately, it is very difficult to estimate the exact amount of energy exhausted (in Joules) for the entire handover process. But the expected amount of energy can be produced to show the effectiveness of the proposed scheme. The purpose of using delay constraints is that real-time traffic is sensitive to delays. Also, the handover delay is a function of delay incurred due to additional processing loads ($d_{load}$) and the signals exchange during the process i.e.

$$d^t = f(d_{load}).$$

Hence, the total energy consumption of any device can be formulated as

$$E_t = E_p(C, T_p, P_k, G_i^k) + E_{HO}(d^k, n_s, n_b) + E_{RF},$$

where $E_p(\cdot)$ and $E_{HO}(\cdot)$ denote the parameters on which $E_p$ and $E_{HO}$ depends, respectively.

At this point, we have completed the description of the system model, channel model best fitted for the scenario, power along with energy consumption model, for TPA. The description for the rest of notations used in the system model is given in table 1. We can now state the problem in our work and the probable approach to overcome the issues, in the following section.
The main goal of the paper is to achieve the maximum energy dissipation spot of moving UE. Since it is an already known fact that UE will consume maximum energy from the serving BS when it is experiencing worst channel conditions. Probably, the maximum energy dissipation spot is the area around handover. This paper aims to design a strategy to trace the pattern of energy for the targeted moving UE from the perspective of finding out the probable region of attack. Although, having more UE’s under the coverage zone of serving BS k will require more power or energy. This strategy will potentially benefit UE in the sense that the highest energy point can be protected through proper mitigation strategies. Thus, enabling secure transmission in the UDN small cell approach in an energy efficient manner.

The energy requirement for the moving UE, which can be defined formally (between two consecutive positions) as the aggregate of the total power consumption for a particular time gap(T), given by

$$E_p^v(v, p, p - 1) = \sum_{k \in B} P_T(P_{k_1}, P_{k_{i-1}}, P_w) \times T(v, p, p - 1),$$  

where T is the time for which we are observing the power consumption and $E_p^v$ depends on the speed of the UE and the separation between $p$ and $p - 1$. Accordingly, the problem can be formulated as follows:

$$\mathcal{P}0: \max \sum_{k \in B} P_T(P_{k_1}, P_{k_{i-1}}, P_w) \times T(v, p, p - 1)$$  

s.t. $\min(s_e) < s_{cth}, \forall k \in \beta, u_i \in \kappa,$ (20a)

$$C_{k_{i}} > C_{E}, \forall k \in \beta, u_i \in \kappa.$$  

### III. PROBLEM FORMULATION AND PROPOSED APPROACH

To elaborate the above illustrated problem a little further, for $\lambda_k = 1$, it can be observed that problem $\mathcal{P}0$ is indeed a mixed non-integer problem, consisting of integer variable $v$, discrete variable $T$ and continuous variable set $s_e$. It is worth mentioning that channel gains $G_i^v$ and $G_{k_i}^v$ expressed in (3) and (6), which are related to our objectives (20b) and (20c), are a function of BSs involvement for a particular UE $u_i$.

Additionally, solving the above mentioned problem $\mathcal{P}0$ becomes intractable for mathematical computations. Presently, we have no existing designs for solving it. We propose an analytic and practical framework, consisting of two separate problems: *as detection of the highest energy point* and *as securing the link using the proposed scheme*. The real-time pattern of the user when multiple picocells are considered is shown in Fig. 3.

To elaborate on the proposed scheme, we first have to design the traces of energy pattern for the moving UEs ($u_i$), in the absence of eavesdropper(s). Next, for a given energy pattern, we consider how to develop the required protection mechanism, in order to further refrain from attacker’s activity. Thus, preventing the moving UE expecting high frequency for handover rates. Fortunately, it is noticeable that the constraints mentioned in $\mathcal{P}0$ are capable of reducing the computational complexity, rather the proposed scheme helps to achieve high accuracy and less false positive rate. Firstly, we will select serving BSs, out of all the active BSs and the moving UEs are spotted and then determine their energy consumption. The proposed detection security scheme will be discussed in detail in the following sections.

### IV. DETECTION ALGORITHM: THERMAL PATTERN ANALYSIS

The main purpose of this section is to design a detection approach, i.e. to determine the probable region of attack for each moving UE. Since UDN is a network in which UEs and APs density is exceptionally very high. Due to which it is practically difficult to measure the amount (damage range) and nature of the attack on the moving UE as it is expected to experience the handovers very frequently. Since it is nearly impossible to provide protection algorithm to each individual. Thus, it is very important to design a detection
algorithm which is versatile and robust for the UDN. So, we propose a scheme which will tackle the UEs growing number within a macrocell unit and able to keep track of next few locations for each moving UE. Such that suitable protection mechanism can be enabled to them beforehand, without much disturbance in the transmission process. With the objective to illustrate the maximum energy consumption region, the thermal pattern analysis can be formulated as

\[
P_0: \max \sum_{k\in\kappa} P_r(P_k, P^p_{k, j}, P_{n}) \times T(v, p, p-1) \quad (21a)
\]

s.t. \( \min(s_c) < S_{c,th}, \forall k \in \beta, u_i \in \kappa, \)

\[
C^p_{k, j} > C^k_{j}, \forall k \in \beta, u_i \in \kappa. \quad (21c)
\]

where the constraint (21a) depends on the power consumption model. It can be seen that the problem (21) is a non-complex combinational problem and finding the optimal solution will not be fitted here. Additionally, the complexity of the proposed scheme cannot be expressed as a closed form expression. At present, there are no existing algorithms to solve the above-stated problem. Simplifying the condition, the complexity of the proposed approach concentrates on the power consumed by the UE for a particular instance. Motivated by this, we could construct a detection approach for securing the transmission in UDN.

Before explaining the details about the algorithm, the pictorialization of UDN can be determined by the coverage distance of small cells, which is straightforward. In general, the close proximity of active AP’s will contribute towards increased data rate and handovers to the moving UEs. In this paper, we adopt the distance covered by moving UE \( u_i \) as the criteria for tracing the energy pattern and then determine the impact of an eavesdropper on the secrecy capacity for a given \( u_i \). Practically, we also assume that serving BS (picocell, BS_1) will serve only a bunch of moving UEs up to a certain distance (\( d_{th} \)) w.r.t. BS_1 and \( d_{th} < R \), where \( d_{th} \): the distance at which channel condition for is \( u_i \) worsens for BS_1 in comparison to BS_2. This results in either the initiation of handover process or depiction about the most likely region of attack. Owing to the fact that eavesdropper will try to overhear the information at any point but the most imputable position would be around the handover region. Thus, proper strategies for protection are required around \( d_{th} \) instead of utilizing the efforts for the entire transmission period. Our algorithm provides us with the embedded strategy for guessing the probable region of attack, which is simpler than any other strategies of detection.

**A. THERMAL PATTERN STRATEGY**

Prior to discussions, the given algorithm is based on assumption that all the information about the current position of UEs is obtained through Global Positioning System (GPS), which is reported back to their serving BSs and the information collected by an individual small cell is managed and monitored by a centralized monitoring system. Hence, we perceive the energy of the UEs for our thermal strategy, in which each UE \( u_i \) first need to inform the BS \( k \) about its channel condition and throughput obtained at position \( p \) after \( t' (t' \ll T) \) slots and then through the (33) derived in Lemma 2, the threshold energy is computed for a particular \( u_i \). At a particular instant \( t \) and \( p \), the maximal position is derived which shows the area of minimal signal strength and is exhaustively computed from (27) in Lemma 1.

To be more specific, the thermal pattern analysis consists of a couple of few search processes:

1. Firstly, for a given UE \( u_i \), if the actual achievable rate \( R_k \) does not satisfy the minimum achievable rate \( R_t \) for \( p \) to the serving BS \( k \) then BS (picocell) \( k^* \) will be introduced as a serving BS for \( u_i \) in place of \( k \) and \( k^* \in \beta \). Also, if the above-mentioned condition (\( R_k > R_t \)) is satisfying but the secrecy capacity \( S_c \) does not satisfy in (8), then there will be probability of attack within \( d^p_{k, i} \) where \( k = \{BS_1\}, k^* = \{BS_2\} \) and \( i = \{u_i\} \) and \( u_i \) will be treated as compromised node/user. In the first search process, all the conditions must be satisfied in order to ensure transmission. Thus, the search process stops after the required target and secure QoS, for all the moving UEs within \( k \) can be guaranteed for UDN.

2. Secondly, if there exist any compromised nodes within \( k \) up to \( d^p_{k, i} \), the report is immediately transferred to the centralized monitoring system. Hence, the attacked node is again traced for the energy pattern through seeking their energy efficiency, while still meeting the criteria for target and secure QoS. If it does not, the area is incorporated under the influence of attack and the HO process will be stopped for \( k^{th} \) BS and thus, a proper preventive measure can be invoked for all the UEs passing through \( d^p_{k, i} \).

We summarize the Thermal pattern analysis in Algorithm 1.

**Algorithm 1** A Thermal Pattern Analysis for detection of probable area of attack in the handover zone under UDN for dense picocell

1. **Initialize:** \( N = \text{random}, X_B = 0, Y_B = 0; \)
2. **Calculate reference \( \{d^p_{k, i}\}, (\forall N \in \kappa); \)
3. **for all** \( N(i.e., i = 1 \to N \& \& i \in \kappa) \)
   4. **Calculate** \( R_t \) (threshold) (as per application demand), where \( i \in \kappa; \)
   5. **repeat;**
   6. **Find** \( j^* = \text{set(moving UEs)}; \)
   7. **end for**
   8. **for all \( j^* \) do**
      9. **if** \( R_k[j^*] > R_t[j^*] \&\& S_c[j^*] > S_{c, th}[j^*] \) **then**
      10. **Mark** \( j^* \) *user “safe”;
      11. **else if** \( R_k[j^*] > R_t[j^*] \&\& S_c[j^*] < S_{c, th}[j^*] \) **then**
      12. **Anomalous behaviour for \( j^* \);
      13. **Compute** \( ee[j^*] \) for all \( p’s \) from (11);
      14. **Match** \( ee[j^*] \) for \( p \) with \( p - 1; \)
      15. **if** \( ee[j^*, p] > ee[j^*, p-1] \) **then**
      16. **Store** the values of \( ee[j^*, p] \);
      17. **end if**
      18. **end if**
      19. **end if**
      20. **end for**
      21. **for all** \( ee[j^*] \) do
22. Find \( p_{j'}^m = \text{pos}(\max^2\{ee(j')\}) \) \( \forall \, p' \)'s;
23. repeat for all \( j' \)’s;
24. end for
25. Output: Set of \( \{p_{j'}^m\}, \forall \, j' \)’s

* \( ee(j',p) \) is the energy efficiency of \( j' \) user at position \( p \)

V. NUMERICAL RESULTS

In this section, we evaluate the performance of our proposed thermal pattern analysis to secure the communication for the moving UEs under dense picocell scenario in UDN. Assuming the cell radius to be 200 m, the two picocells are concentrated with the purpose to retrieve the information about the state of all users. This section is broadly categorized into four major portions. The first part deals with the analysis of performance metrics and channel conditions (e.g. \( \eta_{EE} \) and \( SE \)) and the analysis is performed for the straight and random motion of the user. The second part takes care of interference and secrecy capacity analysis as both acts as a performance limiting parameter. The third part describes the impact on performance with the rise in a speed of the user. The last part comprises of comparison and the real-time testbed analysis of the proposed scheme. The simulation parameters are listed in Table 2.

<table>
<thead>
<tr>
<th>TABLE 2 SYSTEM PARAMETERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Bandwidth</td>
</tr>
<tr>
<td>Picocell coverage range, ( R )</td>
</tr>
<tr>
<td>Path Loss Model [7]</td>
</tr>
<tr>
<td>Picocell BS Transmit Power</td>
</tr>
<tr>
<td>RF Circuit Power Consumption</td>
</tr>
<tr>
<td>Power amplifier efficiency</td>
</tr>
<tr>
<td>Penetration Loss</td>
</tr>
<tr>
<td>RMS delay spread, ( \tau_d )</td>
</tr>
<tr>
<td>Handover Preparation (Decision) Delay</td>
</tr>
<tr>
<td>Handover Execution Time</td>
</tr>
<tr>
<td>Time-to-Trigger</td>
</tr>
<tr>
<td>Path Loss Exponent, ( \alpha )</td>
</tr>
</tbody>
</table>

A. SIMULATION ANALYSIS: PART I

1) Impact of user movement on channel conditions

Owing to the fact that in UDN with the introduction of small cells, the channel fades very slowly reason being 5G has proceeded towards LoS transmission and desired to transmit the information at a very high frequency (~28 GHz). However, the effect of multipath channel propagation would not be dominant for UEs in a dense environment, due to high channel gains which correspond to LoS transmission. Hence, we consider the path loss model for UEs, shadowing loss and Doppler Effect. Thus, assuming the influence of multipath propagation negligible.

Taking \( f_c = 2 \, \text{GHz} \), we need to analyse the network whether channel undergoes Slow Fading or Fast Fading. For this, we need to find out the coherence time \( T_c \) and coherence bandwidth period \( B_c \) and \( T_c \approx \frac{9}{16\delta^2} = 4.47 \, \mu \text{s} \) and, also \( B_c = 2.232 \, \text{KHz} \) for a symbol period, \( T_s = 0.5 \, \text{ns} \). The user moving with 60 kmph (high speed) undergoes Slow Fading as \( T_s \ll T_c \). Hence, in case of UDN architecture, the channel would not vary much due to small distance variation and high frequency of transmission along with high speed of user which is assumed to be constant.

Below Table 3 shows the variation in Doppler shift, \( \Delta f \) as a function of \( v \):

<table>
<thead>
<tr>
<th>TABLE 3 COMPARISON TABLE FOR DOPPLER SHIFTS FOR DIFFERENT VELOCITIES OF USER</th>
</tr>
</thead>
<tbody>
<tr>
<td>( v(\text{kmph}) )</td>
</tr>
<tr>
<td>-----------------------------</td>
</tr>
<tr>
<td>30</td>
</tr>
<tr>
<td>60</td>
</tr>
<tr>
<td>80</td>
</tr>
<tr>
<td>100</td>
</tr>
<tr>
<td>120</td>
</tr>
</tbody>
</table>

If the channels are time-varying and the user is moving, the channel vector \( \mathbf{H}[k] \) at time \( k \), according to Gaussian-Markov model, is given by [36]:

\[
\mathbf{H}[k] \triangleq \alpha' \mathbf{H}[k-1] + \sqrt{1-\alpha'^2} \mathbf{U}[k],
\]

(22a)

where \( \alpha' \in (0,1] \) is the fading correlation coefficient, \( \mathbf{H}[0] \sim \mathcal{CN}(0, \mathbf{I}) \), and \( \mathbf{U}[k] \in \mathbb{C}^M \) has i.i.d entries distributed according to \( \mathcal{CN}(0,1) \), and parameter \( \alpha' \) is given by [36]:

\[
\alpha' = J_0(2\pi\Delta f T_s) \sim 1 - (\pi\Delta f T_s)^2,
\]

(22b)

where \( J_0(.) \) represents the zeroth-order Bessel function. Putting the value of \( \Delta f \) and \( T_s \) from Table 3, we get \( \alpha' = J_0(0.000000628) \approx J_0(0) = 1 \). Substituting the value of \( \alpha' \), in (22a), we get

\[
\mathbf{H}[k] \approx \mathbf{H}[k-1].
\]

(23)

Thus, two important conclusions are drawn from the above study:

1. Firstly, the channel conditions in case of small cell approach experience slow fading in UDN. Hence, in our system model, the response of channel variation in the period of handover (approx. 80 m) is constant in nature.

2. Secondly, there is almost no effect on the value of channel coefficient, due to time-varying nature of channel, for such a high frequency, as a result of Doppler shift.

In the following discussions, we would concentrate on the energy efficiency, Spectral Efficiency \( SE \) and Capacity pattern for a moving UE. The following results are based on two trajectories of a user: 1. Straight, and 2. Random.

2) Study of Energy Efficiency Pattern

Fig. 4 and 5 show the impact of distance \( d_{i,k}^b \) covered by \( u_i \) on energy efficiency when connected to either BS1 or BS2, for straight and random trajectory, respectively. Firstly, we observe that as the \( u_i \) moves away from the serving BS i.e. BS1, the curve for \( EE \) shows an exponential decaying nature.
In a similar way, the pattern for $EE$ shows an exponentially rising curve when $u_i$ starts receiving signals from BS$_2$. This is due to the fact that channel conditions for $u_i$ degrade and the impact of interferences and channel losses become more dominating as the distance between $u_i$ and serving BS (i.e., BS$_1$) gradually increases. As a consequence of which, more energy is required by $u_i$ in order to maintain a sustainable level of the data rate. Even if the ED’s are present, the $R_k$ further reduces which enhances the energy requirement of the UE. Thus, TPA follows a similar trend even if $u_i$ is under the influence of ED. Also, TPA shows the similar trend for every moving user. Specifically, the information leakage may occur more in the region where $u_i$ is about to shift the network i.e. around $d_H$. Additionally, it is worth noting that through TPA, we are able to get the weak spot of attack, $d_H$. Thus, from the attacker’s perspective simply by tracing the pattern of energy requirements for the targeted user, the intensity and the success rate of attack can be improved manifolds. Reason for this is that UDN supports very high data rate support to its UEs and the leakage of information to the eavesdroppers only by degrading the performance would not be feasible here. Hence, only this strategy is capable of providing with the weakest point of attack $d_H$ which would be beneficial to both the eavesdropper as well as for the research perspective. One interesting point can be noted here is that the curves of $EE$ for BS$_1$ and BS$_2$ coincide at a distance of 120 m for Fig. 4 and ~155 m for Fig. 5. The value of $d_H$’s will be different for both the trajectories, rather it depends on the movement of the user but the probable weakest point will definitely occur between $120 \text{ m} < d_H < 200 \text{ m}$. These boundaries will modify according to the network deployment conditions.

![Figure 4. Energy Efficiency variation as a function of distance from BS$_1$ to BS$_2$ for straight path pattern.](image)

From the above analysis, we also conclude that $EE$ and energy consumption by $u_i$ are related to each other. This is due to the reason that with an increase in $EE$ by BS$_2$, the energy requirement for $u_i$ reduces for BS$_2$ in comparison to serving BS (BS$_1$). Hence, $u_i$ will start preparing for handover. In case of random movement of $u_i$, the nature of user will be slightly unpredictable. For analyzing the behavior of random movement of $u_i$, we plot the curve for different positions.

![Figure 5. Energy Efficiency variation as a function of distance from BS1 to BS2 for random path pattern.](image)

3) Study of Spectral Efficiency Pattern

The performance of the TPA is further investigated in Fig. 6 as a function of spectral efficiency for the straight trajectory. First of all, the purpose of using $SE$ is that the results are produced in a numeric form. Hence, spectral efficiency exhibits a similar trend for $EE$, when the separation between $u_i$ and BS$_1$ increases. This is because an increase in distance between $u_i$ and BS$_1$ will degrade the channel conditions as stated earlier. Due to which $u_i$ shows an exponential decay curve for $SE$ when connected to BS$_1$ and coincides with $SE$ of BS$_2$ at a point $d_H = ~160 \text{ m}$. From Fig. 6 and 7, it can be concluded that $SE$ of the user for random movement shows a drastic and abrupt increase in value as compared to the straight trajectory.

![Figure 6. Spectral Efficiency variation as a function of distance from BS$_1$ to BS$_2$ for straight path pattern.](image)

In Fig. 7, the $SE$’s are computed for seven random positions and the same trends can be observed for BS$_1$ as well as BS$_2$ which coincides at a distance of around $d_H = ~160 \text{ m}$. From Fig. 6 and 7, it can be concluded that $SE$ of the user for random movement shows a drastic and abrupt increase in value as compared to the straight trajectory.
4) Capacity Analysis

Through this study, the capacity of $u_i (C_{k,i}^p)$ for various locations relative to BS$_1$ and BS$_2$ are computed and the results are plotted as a function of capacity for the straight and random trajectory of $u_i$.

The curves in Fig. 8 with or without interfere coincide at the same distance i.e. $d_H = 160$ m. It can be concluded that in the presence of an interference signal, the capacity drop could be seen for $u_i$ when connected to BS$_1$. The observation affirms that $d_H$ is the most needful region to implement protection. Since the results are inter-related with the previous performance metrics and the results rely on satisfying the required QoS. Similarly it can be observed from Fig. 9 that at a distance around $160$ m, both the curves coincide which further improves with the increase in $d_{i,k}^p$, $k \varepsilon \{BS_2\}$. This trend is indeed expected here and further reduces when interference power is considered. Thus, in the UDN scenario, interference power plays a major role in reducing the performance of the network. In order to keenly observe the impact of interference, we discuss the impact on the performance of $u_i$ as a function of the density of UEs, in the next sub-section.

B. SIMULATION ANALYSIS: PART II

1) Interference Assessment Model for UDN

In this part, we discuss the common problem of interference associated with UDN, which will limit the performance of the user present under the small cell. However, in typical architecture of UDN, the reduced transmission distance makes it convenient to apply mm-wave communication [34]. Thus, higher network capacity and higher data rate can be guaranteed using mm-wave bands (30-100 GHz). Hence, at higher frequency bands, the influence of interference signals become ineffective. But, due to close proximity and a large density of nearby BSs and interferers make it difficult to combat the impact on the network performance. For this directional antennas can be used to avoid the spatially distributed high density of interferers. As a result, the interference is caused in UDN due to the presence of a large density of users, small cell BSs and hotspot (small network). But, these BSs and users will limit the performance of the system only when it is present close enough to interfere with the transmission. As a result, while assessing the performance of any user either moving or stationary, we will set the area up to which the impact of interferers is computed in the following simulation. Hence, the total interference is a summation of interference from neighbouring users, adjacent (picocell) BSs and hotspots.
The performance is investigated in Fig. 10 as a function of interference power with the rise in UE density for an area of 1256 m² (πr²) where r=40 m. Hence, as depicted in Fig. 10, with an increase in UE density, the interference power increases gradually and slowly but saturates after a certain number of interferers. As the distance between interferers and the serving BS increases, interference power reduces significantly.

Figure 11. Model showing the positions of Eve with different mobility models.

2) Secrecy Capacity Analysis

The previous graphs concentrate only on the estimation of the attacking zones. In this section, we provide an analytic framework where the position of the eavesdropper is kept at one point with simultaneously varying user’s geographical positions. The $S_c$ values are evaluated and plotted for the straight and random trajectory of the user as presented in Fig 12 & 13, respectively, by assuming three random locations of eavesdropper marked as $\beta_1$, $\beta_2$ and $\beta_3$. In order to have a clear overview where the eavesdropper is exactly positioned refer to Fig. 11. On the basis of $S_c$ analysis from (8), we have found that $S_c$ for $\beta_2$ is greater than $\beta_3$, followed by $\beta_1$.

Figure 12. Probability of Spoofing with respect to Secrecy Capacity vs Distance for three different positions $\beta_1$, $\beta_2$ and $\beta_3$ (Straight path).

In the case of random path model, the $S_c$ changes in a graded index manner i.e. channel conditions will not change point-to-point. But for straight movement, path loss decays in an exponential manner.

Figure 13. Secrecy Capacity versus distance covered by user, evaluated for three different positions of eavesdropper by assuming random trajectory.

3) Theoretical Analysis and Comparison

In order to observe the potential benefits of TPA, we perform a theoretical as well as numerical analysis under a realistic multicellular and dense scenario. The energy consumed by the moving device as a function of $d_{ik}^p$, $k \in \{BS_i\}$ is considered as the performance metric for studying the TPA. Since the study of TPA is associated with the security issues encountered by moving user in the dense UDN environment. Thus, our proposed algorithm (TPA) proves to be efficient as the approach can detect the presence of attacker (or ED) in the handover region and other regions of the cell coverage, by matching the real-time energy demand with the threshold energy consumption in that area.

Compared to [17], TPA is significantly successful in detection of attacker’s presence, resulting in more accurate performance. Although, through SNR, the channel variations could be easily noticeable. Hence, the chances of False Positive rate (FPR) arises by virtue of worst channel condition. As a result, the accuracy of the scheme, [17] reduces in comparison to TPA. Initially, we assume that the ED is present somewhat near to handover zone but in the practical case study, it could influence the performance of the legitimate user at any location. Hence, in [17], the chances for error propagation is more dominant in reference to TPA. Also, without knowledge about CSI of ED, it is nearly impossible to explicitly determine the area of attack.
Therefore, accuracy is used as the metrics to test the suitability and reliability of the proposed scheme and it can be defined as the ratio of the number of successful attempts to the total number of attempts.

\[
\text{Accuracy} = \frac{\text{No. of successes}}{\text{Total no. of attempts}} \times P_{\text{hit}} \times 100, \tag{24}
\]

where \( P_{\text{hit}} \) denotes the probability that the \( X \)-approach is effective in interpreting the presence of the intruder. Hence, in our approach, we have taken the number of the attacker (or ED) attempts to be 5. Fig. 14 shows the comparison graph of the proposed algorithm (TPA) with [17]. The analysis is performed for 10 iterations. But with each iteration, the ED location varies and the expected accuracy is predicted for TPA and [17]. It can be inferred from the graphical analysis that with every iteration, the accuracy varies for both the algorithms. But, the work in [17] achieves a maximum accuracy of \( \sim 60\% \) or even less. Additionally, TPA outperforms the approach used in [17] for almost every iteration. Hence, the proposed methodology is successful in every situation either created by the network during transmission or attacker. Unfortunately, until now, there is no study related to tracing pattern of moving users for the problem mentioned in this paper.

**C. SIMULATION ANALYSIS: PART III**

1) Impact of user mobility on performance

The impact of variation in velocity of the user on the SIT\(^3\) and energy consumed during transmission is presented in Fig. 15. It is noteworthy that for a fixed target rate, \( R_t = 2 \, \text{Mbps} \) (HD video Application, [42]), the SIT gradually decreases exponentially with the rise in \( v \). The decrement of SIT is very sharp when \( v \) reaches a maximum value of 120 km/h. Here, the SIT is analogous to transmission duration. However, energy consumed is related to two parameters, 1) dense scenario and 2) Channel conditions and multi-path fading. In the latter case, the complexity arises with the worsening of channel conditions of the user. But it is difficult to estimate the corresponding energies at the present stage. That is why we opted for dense scenario and further limiting our work to transmission energy only. It is also noteworthy that the similar trend will be observed for different \( R_t \)'s. Also, the energy poses the lowest value, when \( v \) reaches 120 km/h. Additionally, from the previous results, we obtain \( d_H = 160 \, \text{m} \) and all the computations are based on this assumption.

![Figure 14. Accuracy vs No. of iterations obtained through proposed approach (TPA) and [17].](image)

![Figure 15. Energy consumed and SIT vs speed of user](image)

2) Experimental Setup and Explanations

**Description:** To analyze the proposed approach, the real-time testbed is structured to investigate the interfacing of the algorithm with the actual world. Fig. 16 illustrates the experimental setup used for the assessment of the values in the TPA approach. We designed a prototype to examine the working of the algorithm, before integrating it on a large-scale. From Fig. 16 (a), we integrate GSM Module and Temperature sensor (LM35) with Arduino 1.8.5. Therefore, three main types of programming modules are present in this hardware setup for obtaining the relationship between the simulation studies with actual real-time analysis. Here, LM35 is not integrated directly with the mobile device, due to the limitation in their coverage area and also, the sensor is interfaced with the board through a wired link. Thus, restricting the movement of the device and sensor.

On a contrary, the sensing unit plays a major role in extracting the information from the surroundings. Therefore, the configuration of the sensing unit is of utmost importance, in order to obtain precision in the results. We have maintained a room temperature of 25°C for conducting the tests. But in an actual environment, the moving device is mainly present inside the moving vehicle, where the

\(^3\) Session initiation time (SIT) is defined as the time taken by the user to reach the handover condition with respect to reference position and in this case \( d_H = 160 \, \text{m} \).
temperature solely depends on the type of vehicle used for travelling. In case of pedestrian motion $v \leq 4 \text{ kmph}$, the device may be present in the vicinity of office, walking inside the residential area etc. With this much speed, it is quite possible and easy to predict the next few probable locations. Hence, another important parameter of concern is the direction of the user for the next few instances. This will ease in computing the threshold for energies for the next instance, even if the speed of user unexpectedly rises from low to high. Along with the above described setup, a proper training model is required to be designed, which will automatically acquire the desired range of energies. However, the designing of the training model can be left for the future scope as it is difficult to design the model at the present stage, which further requires exhaustive studies.

**Case Study:** To overcome the aforementioned shortcoming of moving users in UDN (as described in Section I), we design an approach to trace the pattern of energy and thus, provisioning them with confidentiality which is the prioritized task as far as real-time deployment of UDN is concerned. All the components are assembled together as shown in the block diagram (Fig. 16 (e)). Prior to this, the proper working knowledge about the modules is required before proceeding towards the assembling stage.

Initially, the temperature sensor will sense the analog information from the surroundings which includes temperature maintained in the lab, heat radiated by the body nearby and climatic conditions. Here, we consider two operational modes of the sensor (LM35) namely 1) Normal Mode, and 2) Anomaly mode. After every $t$ seconds, the sensor will provide the sensed information (i.e. the current temperature $T_p$ at $p$ position) to the Arduino Kit, which is independent of the operational mode. Further, the processor will decode and compare the processed information with the predefined threshold value ($Th$), in a needful course. The threshold value is decided only after observing the internal and external factors. The external factors include the temperature of the testing area, heat radiated by the body in close contact with the object (i.e. mobile device) and so on, as explained earlier. The factors which contribute to the internal factors are running application(s) like audio or video, intruder, and high channel losses. Although, the sensor is not integrated with the device, particularly for observing the impact of the intruder. In this work, the laser ($\sim 0.1 \text{ or } > 1000 \text{ mW}$) could act as an intruder and thus, the issue can be resolved in this way. The temperature could be raised by only a few degrees ($1 -2\degree C$) when high intensity beam of the laser is projected for only a few seconds. Furthermore, as long as $T_p < Th$, the alert will not be generated to the owner. But, once the boundary limits are crossed, the report will be sent either in the form of a text message (SMS) or alarm. As it has been already mentioned that it is a prototype study and the actual values could deviate slightly or even more from the observed scenario here.

**Applications:** In this section, we discuss the potential applications of this proposed scheme (TPA). The main aim of introducing this scheme is to enable protection to the users under motion. Sincerely speaking, this type of methodology could be applicable to all the devices either moving or stationary. However, we have limited our work for only one problem of frequent handovers in UDN. But the similar approach could be extended and simultaneously modified for heterogeneous devices, working in different domains. As it
has been an already known fact that 5G is a collaboration of innumerable number of heterogeneous networks working on different protocols. More specifically, security is a major concern and listed among the prioritized condition. However, the application of the proposed scheme is not limited but can be used for the defense purpose for monitoring the critically acclaimed areas, where security cannot be compromised at any cost. For defense applications, the sensors are deployed in a random fashion and any sort of anomaly either in the form of the sudden rise of temperature due to the presence of intruder could be responded to the reporting unit in an intelligent manner. Furthermore, the sensors could be used to monitor the activity in the border areas. Hence, a proper mechanism needs to be designed for differentiating the anomaly behavior of an intruder with the innocent person or animal. In addition, to further enhance the reliability of the scheme, the activity of the sensitive region can be double checked with the image obtained either from the drone or night-vision device, which requires extensive image processing tasks.

D. SUMMARY OF OBSERVATIONS AND LIMITATIONS
The thermal pattern analysis based framework designed for UDN environment significantly helps in tracking the moving users. This framework is developed to estimate the energy pattern pertaining to movement of the user. Considering various channel losses and speed influence on performance. Despite many advantages, there are few limitations of the TPA scheme which follows. Firstly, it is very important for the monitoring center to bifurcate between two cases i.e. eavesdropper is present or not. However, there may be a condition where the quality of the channel deteriorates due to the sudden rise in the number of obstacles. As a consequence, the SNR and EE drop which further leads to an increase in energy consumption. So, in order to meet the given target QoS, BS is required to supply more power to the user and thus, computational complexity suddenly increases. Secondly, speed acts as a limiting factor as it is difficult to trace the user and generate an energy pattern, with high mobility. To end this, practically the temperature radiated by mobile device is very low and sincerely, it is very difficult to estimate the small variation, for defense purpose. For such a case, the temperature of the surrounding bodies either living or non-living like weapons or humans can be considered to observe the changes in the value.

VI. CONCLUSION AND FUTURE WORK
In this paper, a thermal (or energy) pattern based low-security location estimation technique is presented for high handover rates problem in UDN environment. The solution to handover related security issue focuses on energy and spectral efficiency with different types of user’s trajectories including straight and random. The thermal pattern based tracing method is useful in finding out the low-security zone and the impact on the performance is further validated by assuming random locations of eve. Our results have shown that we have been able to trace the low-security zone with greater accuracy. This paper has provided with a novel method to estimate the real-time energy requirement of any device which further aids in finding the most probable area of attack, by comparing against a predefined threshold. It has been also concluded from the analysis that the presence of neighbouring users will also raise the energy consumption of the moving user. But the considerable effect will be seen in case of low mobility users in regards to the probability of attack and energy required during transmission. Hence, the power required for the computation process increases radically. This proposed method is unique in comparison to other defined detection algorithms which requires extensive computational capability. Despite handover related security concern for UDN, there are other issues which are yet to be resolved by the researchers. In addition, the proposed approach provides a platform for the researchers to carry out the study in the real world by including all channel losses and their corresponding energy requirements.

APPENDIX

PROOF OF LEMMA 1
Consider a scenario as shown in fig. 2. In order to calculate the cross-over distance from a set of $d_{i,k}$’s for $u_i$ such that proposed scheme can obtain the highest energy requirement region, we need to find the first order derivative of multiple of interference and path loss from (6). The crossover point can be termed as $d_H$ as mentioned earlier, which represents the probable position for handover initiation. Let $X = P_l, I^p$ be the product of channel gain and total interference experienced by $u_i$. Putting $P_l = d_{i,k}^p, \alpha$ represents the path-loss exponent, we get

$$X = d_{i,k}^p I^p, \Rightarrow \log X = \alpha \log d_{i,k}^p + \log I^p.$$  

(25a)

Performing the first-order derivative of $X$ with respect to distance, we have

$$\frac{1}{X} \frac{dX}{dd_{i,k}} = \frac{\alpha}{d_{i,k}} + A,$$  

(26)

Equating the above term equal to zero ($\frac{dX}{dd_{i,k}} = 0$), we get

$$\frac{\alpha}{d_{i,k}} + A = 0 \Rightarrow d_{i,k}^p = -\frac{\alpha}{A},$$  

(27)

where $A = \frac{dI^p}{dd_{i,k}}$ and again differentiating (25b) with respect to $d_{i,k}^p$, we get

$$\frac{dX^2}{dd^2_{i,k}} = \frac{\alpha}{d_{i,k}^p} \left(\frac{dX}{dd_{i,k}}\right)^2 + \left(\frac{dX}{dd_{i,k}}\right) A,$$  

(28)

Putting the value of $d_{i,k}^p = -\frac{\alpha}{A}$ in the above equation and after solving, we get

$$\frac{dX^2}{dd^2_{i,k}} = A, I^p d_{i,k} (1 - \alpha).$$  

(29)

The resultant equation after second-derivate will be less than zero i.e. $\frac{dX^2}{dd^2_{i,k}} = AI^p d_{i,k} (1 - \alpha) < 0$, as $\alpha > 1$ is greater than 1. So, $(1 - \alpha)$ will always result in negative
value. Thus, \( d_{ik}^p = -\frac{\sigma}{A} \) is the maximal point at which \( X = d_{ik}^p \) attains a minimum value.

**PROOF OF LEMMA 2**

For a moving user \( u_i \), the energy requirement can be defined as the product of total power consumption and time for which transmission occurs. Hence, mathematically, the energy requirement for \( u_i \) at \( p \) can be written as

\[
\mathcal{E}_p = P_k \cdot T_p,
\]

where \( P_k = 1/\eta \cdot p_{ik}^k + n_A P_w \) is the total power consumed by \( u_i \) for duration \( T_p \).

\[
\mathcal{E}_p = \left( \frac{C_i (TP \times B_{-1})}{2} \right) \frac{p_i^2}{g_k^i} \tag{30}
\]

where \( p_{ik}^k \) is the aggregate capacity of \( u_i \) from \( i = 0 \) i.e. reference position to \( i = p \). Hence, the above-derived equation can be used directly to estimate the threshold value of energy requirement and the computed results can be readily compared with the simulated real-time values.

**REFERENCES**


