An Efficient Energy Based Secret Key Generation Approach for Jamming Attacks

MIRZA BURAN BAIG[1], MD. ATEEQ UR RAHMAN[2]
[1]PG Scholar, Dept of CSE, SCET, Hyderabad, TS, India
[2]Professor & HOD, Dept of CSE, SCET, Hyderabad, TS, India

Abstract: Sticking assaults speak to a basic defenselessness for remote mystery key age (SKG) frameworks. In the present examination, two counter-sticking methodologies are explored for SKG frameworks: to start with, the work of vitality reaping (EH) at the genuine hubs to transform some portion of the sticking force into helpful correspondence power, and, second, the utilization of channel bouncing or power spreading in piece blurring channels to diminish the effect of sticking. In the two cases, the antagonistic collaboration between the combine of honest to goodness hubs and the jammer is detailed as a two-player zero-whole amusement and the Nash and Stackelberg equilibria (NE and SE) are described diagnostically and in shut frame. Specifically, on account of EH collectors, the presence of a basic transmission control for the honest to goodness hubs permits the full portrayal of the amusement's equilibria and furthermore empowers the entire balance of the jammer. On account of channel bouncing versus control spreading systems, it is demonstrated that the jammer's ideal procedure is dependably control spreading while the honest to goodness hubs should just utilize control spreading in the high flag to-impedance proportion (SIR) administration. In the low SIR administration, while staying away from the jammer's obstruction winds up basic, channel bouncing is ideal for the true blue hubs. Numerical outcomes exhibit the proficiency of both counter jamming measures.

Index Terms: Secret Key Generation, Jamming, Energy Harvesting, Channel Hopping, Zero-Sum Game.

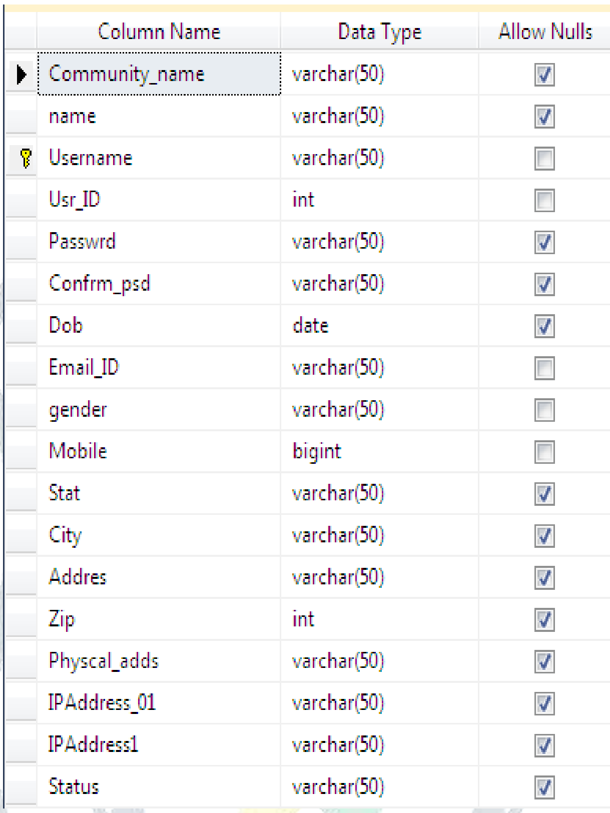
I. INTRODUCTION

Secret key generation (SKG) from shared at two remote locations has been throughly studied [3]–[12] and has been extended to unauthenticated channels [13], [14]. SKG techniques have also been incorporated in protocols that are resilient to spoofing, tampering and man-in the- middle active attacks [15], [16]. Still, such key generation techniques are not entirely power full against active adversaries during the advantage distillation phase. Disaffirmation of service attacks in the form of jamming are a known vulnerability of SKG systems; in [17], it was confirmed that when increasing the jamming power, the revision rate normalized to the rate of the SKG increases sharply and the SKG process can in essence be brought to a stop. As SKG techniques are currently being assosiated for applications such as the Internet of things (IoT) [18], the study of more relevant counter-jamming approaches is timely. Jamming in wireless communication systems has been examined using game theoretic tools [19]–[27]. Contradictory to our work, these earlier studies focus on performance metrics that are based on the legitimate nodes' signalto- interference-plus-noise ratio (SINR) [19]–[25] and do not incorporate physical-layer security constraints at all, or are based on the secrecy capacity [26], [27]. The secrecy capacity is essential different than the SKG capacity considered in this work; the measures the maximum rate at which both confidential communication is possible, while the latter represents the maximum rate at which a common secret key can be used from the observation of correlated sequences at two remote locations [28]. In the past, two main counter-jamming approaches have been considered: direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) [29], [30]. The impact of power constrained jammers can be limited because their optimal strategy has been proved to be the spreading of their available power over the entire bandwidth. However, DSSS and FHSS systems require a secret to establish the spreading sequence or the hopping pattern at Alice and Bob; as such, they are not directly applicable to SKG systems that on the contrary seek to establish a secret key. Attempting to resolve this contradiction and reconcile DSSS and FHSS with SKG, unorganised frequency hopping and spreading techniques have recently been investigated in [31], [32]. The main idea behind the proposed methods was for the selection of the hopping/spreading sequences, at the cost of reducing the achievable rates for secret key establishment. However, in uncoordinated hopping/spreading techniques there are minimum requirements regarding the length of the pseudorandom sequences employed.

As a result, accounting for the strict bandwidth specifications of fourth and fifth generation networks, the use of long pseudorandom sequences can be a limiting factor. Investigating different counter jamming approaches based on the use of channel hopping or power spreading over multiple orthogonal subcarriers, e.g., orthogonal frequency division multiplexing (OFDM) systems [19], [21], is timely and offers an interesting alternative to [31], [32] as in OFDM systems there is no need for organising of the remote nodes. Furthermore, although in [31], [32] the numerical investigations focused on the throughput, a Media Access Control (MAC) layer amount, while investigating physical layer security SKG frameworks the standard approach is to use the SKG limit (a physical layer amount). On an alternate note, cutting edge terminals are probably going to be upgraded with numerous new highlights that could demonstrate significant in ensuring against sticking. For instance, more noteworthy vitality self-governance abusing vitality gathering (EH) approaches [33], [34] is being inquired about for frameworks, for example, remote sensor systems for IoT applications. In this way, it is intriguing to explore whether EH could be used as a counterjamming strategy by abusing the reaped sticking force to improve the nature of the authentic correspondence. Spurred by the above, in the present work we propose two novel methodologies for mitigating the effect of sticking in SKG frameworks. In both methodologies, we show the association between the honest to goodness hubs and the antagonistic jammer as a two-player zero-total diversion in which the SKG limit assumes the part of the utility capacity. We research two non-cooperative arrangements: the Nash equilibria (NE), when the two players settle on their choice at the same time and the Stackelberg equilibria (SE), when the honest to goodness hubs have leverage and pick their procedure first while foreseeing the jammer's reaction. In the initial segment of this commitment, we ponder frameworks in which the true blue hubs are outfitted with EH capacities and inspect whether this additional usefulness is valuable in appropriating sticking assaults. We center around time exchanging EH conventions [34]: for a small amount of time the honest to goodness hubs work in EH mode and change to the SKG technique for the rest. To the best of our insight, this is among the primary attempts to examine EH as a counter-sticking methodology with the special case of [25].

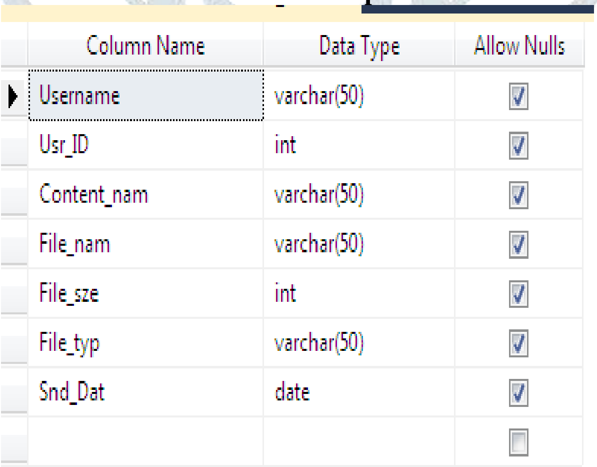
II. DATABASE DESIGN

TABLE I: Access



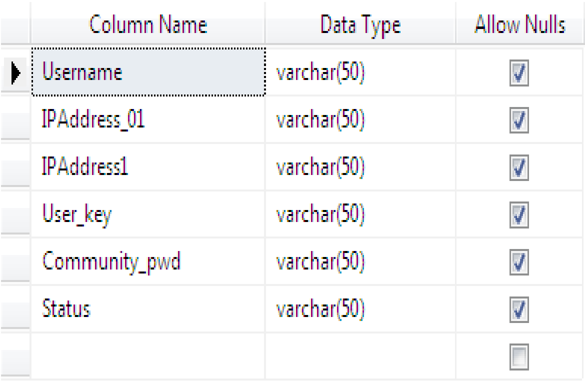
	Column Name	Data Type	Allow Nulls
▶	Community_name	varchar(50)	☑
	name	varchar(50)	☑
🔑	Username	varchar(50)	□
	Usr_ID	int	□
	Passwrd	varchar(50)	☑
	Confrm_psd	varchar(50)	☑
	Dob	date	☑
	Email_ID	varchar(50)	□
	gender	varchar(50)	□
	Mobile	bigint	□
	Stat	varchar(50)	☑
	City	varchar(50)	☑
	Addres	varchar(50)	☑
	Zip	int	☑
	Physcal_adds	varchar(50)	☑
	IPAddress_01	varchar(50)	☑
	IPAddress1	varchar(50)	☑
	Status	varchar(50)	☑

TABLE II: File Upload



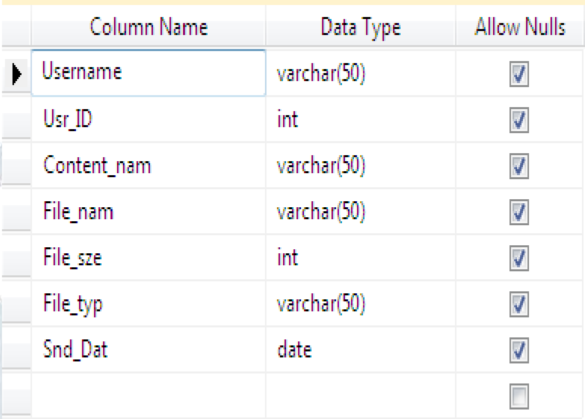
	Column Name	Data Type	Allow Nulls
▶	Username	varchar(50)	☑
	Usr_ID	int	☑
	Content_nam	varchar(50)	☑
	File_nam	varchar(50)	☑
	File_sze	int	☑
	File_typ	varchar(50)	☑
	Snd_Dat	date	☑
			□

TABLE III: User Details



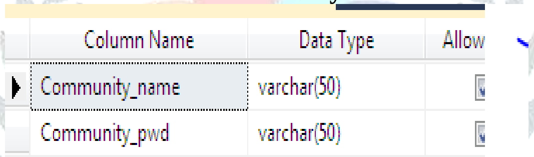
Column Name	Data Type	Allow Nulls
Username	varchar(50)	☑
IPAddress_01	varchar(50)	☑
IPAddress1	varchar(50)	☑
User_key	varchar(50)	☑
Community_pwd	varchar(50)	☑
Status	varchar(50)	☑
		☐

TABLE IV: File Store



Column Name	Data Type	Allow Nulls
Username	varchar(50)	☑
Usr_ID	int	☑
Content_nam	varchar(50)	☑
File_nam	varchar(50)	☑
File_sze	int	☑
File_typ	varchar(50)	☑
Snd_Dat	date	☑
		☐

TABLE V: Community Password



Column Name	Data Type	Allow
Community_name	varchar(50)	☑
Community_pwd	varchar(50)	☑

III. SKG SYSTEM MODEL IN THE PRESENCE OF A JAMMER

The pattern SKG framework demonstrate with two honest to goodness hubs, meant by Alice and Bob and a solitary enemy, indicated by Eve, is delineated in Fig. 1. Regularly, the SKG procedure comprises of three stages [4], [6]. In the main stage, alluded to as shared haphazardness refining, Alice and Bob watch subordinate arbitrary factors meant by YA; YB while a spy, alluded to as Eve, watches YE. In remote channels, a promptly accessible wellspring of shared haphazardness is the multipath blurring because of the correspondence of the remote medium amid the channel's lucidness time [10]– [12]. Here, we center only around shared irregularity extraction from Rayleigh blurring coefficients. In the following two stages, known as data compromise and protection enhancement, side data V is traded amongst Alice and Bob, produced by comparing encoders. Toward the finish of the SKG procedure, a typical key is removed at Alice and Bob with the end goal that, for any , the accompanying proclamations hold [8]: where H(K) indicates the entropy of the key K and I(K;V) means the common data amongst K and V. The principal imbalance shows that the SKG procedure can be made blunder free;(2) guarantees that the trading of side data through open talk does not release any data to meddlers; while(3) builds up that the produced keys achieve greatest entropy (i.e., are uniform). Under the three conditions, an upper bound on the rate for the age of mystery keys is given by [3],[4]. Accepting rich multipath conditions, the decorrelation properties of the remote channel over short separations can be abused to guarantee that Eve's perception YE is uncorrelated with YA and YB [7]– [11]; for this situation, the SKG limit is given by [3, Sec. II](4)

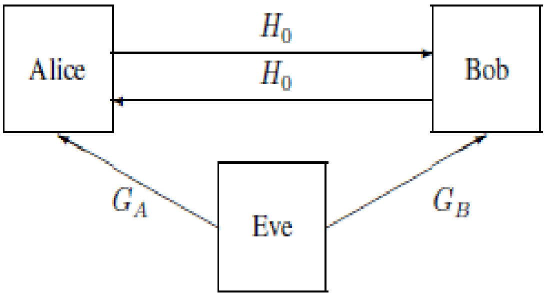


Fig.1. SKG system model with two legitimate nodes and a single adversary.

We accept that this remains constant in whatever is left of this investigation and consider the SKG limit above to be the central execution metric. SKG in Rayleigh blurring channels has been broadly investigated, e.g., [7], [8]. In these works, it was accepted that Alice and Bob trade unit test signs to energize the blurring channel and acquire particular perceptions YA and YB with where H0 signifies the blurring coefficient in the connection between the authentic hubs, demonstrated as a zero mean Gaussian arbitrary variable, and, ZA and ZB display the impact of AWGN and signify autonomous and indistinguishably dispersed (i.i.d.) Gaussian irregular factors . Utilizing this documentation, the SKG limit has been communicated as [8]: In this work, we accept that Eve is never again a latent meddler yet a noxious jammer. To incorporate sticking assaults in the above model, we think about the accompanying expansion: expecting that Alice and Bob trade consistent test signals [8] with control and that Eve transmits steady sticking signs [17] with control. The blurring coefficient in the connection amongst Eve and Alice is meant by and in the connection amongst Eve and Bob by. For straightforwardness and without loss of simplification, the commotion factors ZA and ZB are expected to have unit change, i.e., are demonstrated as i.i.d. Gaussian irregular factors .Under these presumptions, a basic estimation uncovers that the SKG limit can be communicated as an element of p and: By examining the main request subsidiaries of (8), we presume that C(p;) is an entirely expanding capacity of p for any settled , and an entirely diminishing capacity of for any settled p. This infers the honest to goodness hubs will transmit at full power P to boost the SKG limit, though the jammer will likewise transmit with full energy to limit the SKG limit. Likewise, it is an entirely curved capacity concerning (w.r.t.) for any settled p > 0 as its second subordinate w.r.t. is entirely positive.

IV. ENERGY HARVESTING AGAINST JAMMING

With a specific end goal to consider EH as a counter-sticking measure, we center around a period exchanging EH plot [34], i.e., we expect that every transmission interim of span T is isolated in two sections. In the principal time of span being the part of T committed to EH), both Alice and Bob work in EH mode with effectiveness in the second time of term , the real hubs work in SKG mode utilizing the general accessible power (counting gathered power). For straightforwardness, we expect that the vitality gathered can be put away in a battery with no flooding issues (boundless capacity) [35]. Moreover, to facilitate the scientific inference and by guaranteeing symmetry in the vitality reaped at Alice and Bob we accept that (the Eve-Alice and Eve-Bob joins have square with fluctuation). Given the above contemplations and accepting that the vitality reaped by Alice and Bob is direct in the gotten RF control [34], [36]: The reaped control for each real hub per transmission interim can be communicated as Where is a raised expanding capacity of . Hence, the SKG limit is given by: With control requirements. A straightforward investigation of (11) uncovers that this situation is a speculation of the standard SKG setting. Without a doubt, if the true blue hubs choose not to collect vitality, i.e. , is acquired for . In the model with EH, the genuine hubs can augment ~u by tuning the extra factor . Notwithstanding, it is never again direct that the jammer ought to transmit with the greatest accessible power just like never again monotonically diminishing in Non-agreeable diversion hypothesis gives the normal structure to think about the antagonistic association between the honest to goodness hubs and the jammer. Albeit amusement hypothesis has just been abused in physical layer security issues, e.g. [26], [27], to the best of our insight, this work is among the first to examine EH as a successful intends to neutralize on sticking assaults.

A. Jammer Neutralization

Before presenting the diversion structure, we mention two vital objective facts in regards to the SKG utility in (11) and talk about their suggestions. This novel outcome demonstrates that the sticking obstruction, which is ordinarily thought as being unsafe to the authentic correspondence, can be abused and changed into valuable power through EH. In the event that Alice and Bob transmit with precisely pth, the jammer ends up aloof between every one of its decisions and has no enthusiasm for currently sticking the transmission. The important conditions for the jammer balance are formalized beneath.

Recommendation 1: The ideal methodology for the genuine hubs that amplifies the SKG utility while guaranteeing that the jammer has no enthusiasm for currently sticking the transmission is given by:

$$\arg\min_{\gamma\in[0,\Gamma]} \tilde{u}(p,\tau,\gamma) = 0, \text{ if } p < p_{th}(\tau) \quad (1)$$

$$\arg\min_{\gamma\in[0,\Gamma]} \tilde{u}(p,\tau,\gamma) \in [0,\Gamma], \text{ if } p = p_{th}(\tau) \quad (2)$$

$$\arg\min_{\gamma\in[0,\Gamma]} \tilde{u}(p,\tau,\gamma) = \Gamma, \text{ if } p > p_{th}(\tau) \quad (3)$$

B. Game Formulation and Nash Equilibria

The communication between the authentic hubs and the jammer is formalized as a two-player zero-entirety amusement, characterized as the tuple in which the players may be: player L speaking to the honest to goodness hubs (Alice and Bob go about as a solitary player) on one side, and player J, the jammer, on the other. The activity (p; _) of player L lies in the set A~L = [0; P] _ [0; 1], and the activity of player J lies in the set A~J = [0; □]. The goal of player L is to boost the SKG utility ~u(p; _;) given in (11), while player J goes for limiting it. The two players are foes and the ideal technique of one player relies upon the decision of their adversary and can't be resolved singularly. In such intelligent circumstances, the NE [37] is the regular arrangement idea. Naturally, a profile (pNE; _NE; NE) 2 A~L _A~J is a NE if none of the players can profit by straying from this profile realizing that their adversary plays likewise. Thus, NEs are framework expresses that are steady to one-sided deviations.

IV. CHANNEL HOPPING VS. POWER SPREADING IN BF AWGN CHANNELS

In the event that the honest to goodness hubs don't have EH abilities, we explore yet another approach to protect against sticking by accepting that the authentic hubs can utilize channel bouncing or power spreading systems over numerous orthogonal subcarriers. For this, we sum up the framework display (6) and (7) to a N-BF AWGN channel. Alice's and Bob's perceptions on the I-th subcarrier – indicated by separately – are communicated as: where the blurring coefficient in the connection amongst Alice and Bob on the I-th subcarrier is indicated by Hi, in the connection amongst Eve and Alice by GA;i and in the connection amongst Eve and Bob by GB;i. We accept that the blurring coefficients are i.i.d. Gaussian irregular factors with . Notice that the blurring coefficients are expected to have similar insights. This supposition is advocated, since, comprehensively, narrowband blurring relies upon the transfer speed (which is the same for all subcarriers) and not on the focal recurrence (not at all like wideband blurring or huge scale blurring) [38]. Moreover, the commotion factors ZA;i and ZB;i are thought to be i.i.d. Gaussian zero mean unit change arbitrary factors. At last, Alice and Bob trade consistent test signals [8] with control pi and that Eve transmits steady sticking signs [17] with control I on the I-th subcarrier so the accompanying normal power limitations are satisfied2 [19], [21]: When transmitting over the whole range, the decision of the uniform power designation is persuaded by the way that the hubs don't have the foggiest idea about their real channel picks up and that their measurements are indistinguishable over all recurrence transporters. The jammer is ideal and limits the general SKG utility. More broad power portion strategies can be considered in future examinations. From a usage perspective for the proposed channel jumping and power spreading techniques, we look at that as an OFDM transmitter with a standard opposite quick Fourier change (IFFT) piece is utilized. In channel bouncing mode, everything except a haphazardly picked IFFT input are set to zero. No coordination with respect to the picked channel bouncing or spreading alternatives is required amongst transmitting and accepting terminals. This is conceivable if wideband gathering is utilized by all gatherings, permitting transmitting terminals to freely pick their techniques without coordination with the accepting terminals. Such a wideband gathering of the N orthogonal subcarriers can be effectively actualized utilizing a standard FFT based OFDM recipient. Where the standardization 1N represents estimating the SKG limit in bits/s/Hz. In (23), the principal term relates to the case in which Alice (resp. Sway) jumps on subcarrier I and the jammer jumps on an alternate subcarrier; the second term to the case in which Alice (resp. Bounce) and the jammer both jump on subcarrier I; the third term to the case in which Alice (resp. Weave) bounces on subcarrier I and the jammer spreads; the fourth term to the case in which the Alice (resp. Bounce) spreads and the jammer jumps on subcarrier I. At last, the last term relates to the case in which they both spread their energy.

A. Amusement Formulation and Nash Equilibria

We show the focused cooperation between player L and J as the accompanying zero-aggregate diversion, where the result is given in (23). The activity sets of the players are the probabilities of channel bouncing and power spreading:

$$\begin{aligned}\hat{\mathcal{A}}_L &= \left\{\alpha \in [0,1]^{N+1} \middle| \sum_{i=1}^{N+1} \alpha_i = 1\right\},\\ \hat{\mathcal{A}}_J &= \left\{\beta \in [0,1]^{N+1} \middle| \sum_{i=1}^{N+1} \beta_i = 1\right\}.\end{aligned} \quad (4)$$

As we have argued in the previous section, the natural solution in such a strategic interaction without cooperation among the opponents is the NE. To derive the game's NE, let us introduce a finite discrete game ^ $\hat{\mathcal{G}}^{D} = \{\hat{\mathcal{E}}_L, \hat{\mathcal{E}}_J, \hat{u}(\alpha,\beta)\}$ with action sets defined as $\hat{\mathcal{E}}_L \equiv \hat{\mathcal{E}}_J = \{e_1, \ldots, e_N, e_{(N+1)}\}$.

V. RESULT

Results of this paper is as shown in bellow Figs.2 to 6.

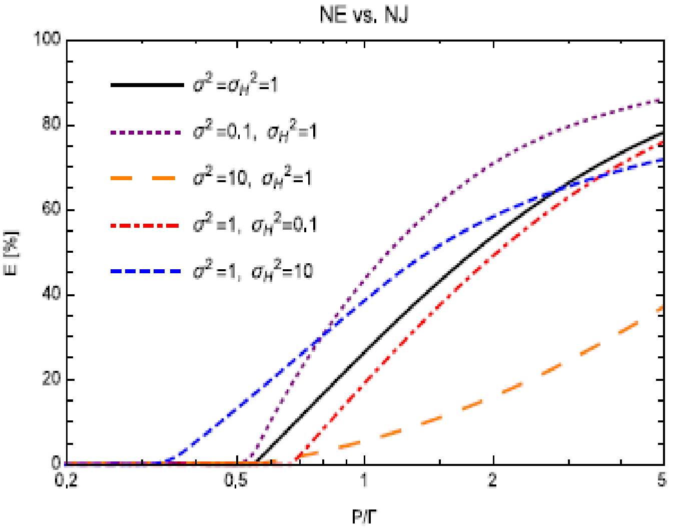


Fig.2. Relative utility gain at the NE vs. N $E = (C^{NE} - C^{NJ})/C^{NE}$ as a function of P=□ _ 0 for _ = 0:7.

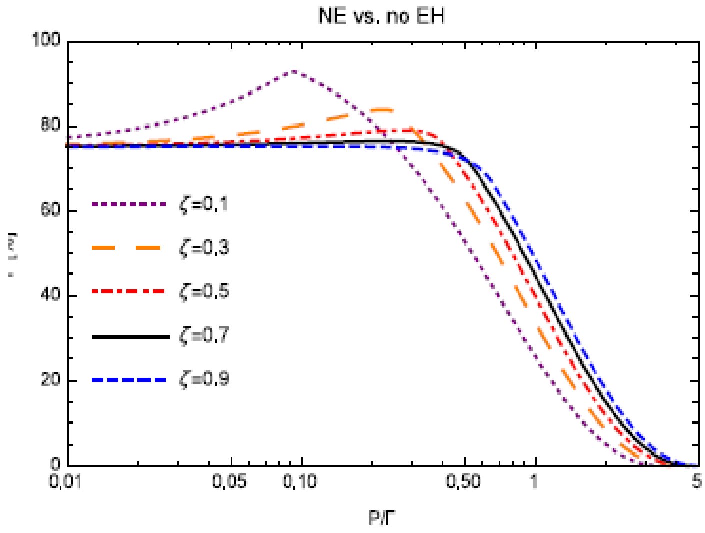


Fig.3. Relative utility gain at the NE vs. no EH: $F = (C^{NE} - C^{noEH})/C^{NE}$ **as a function of** $P/\Gamma \geq 0.$

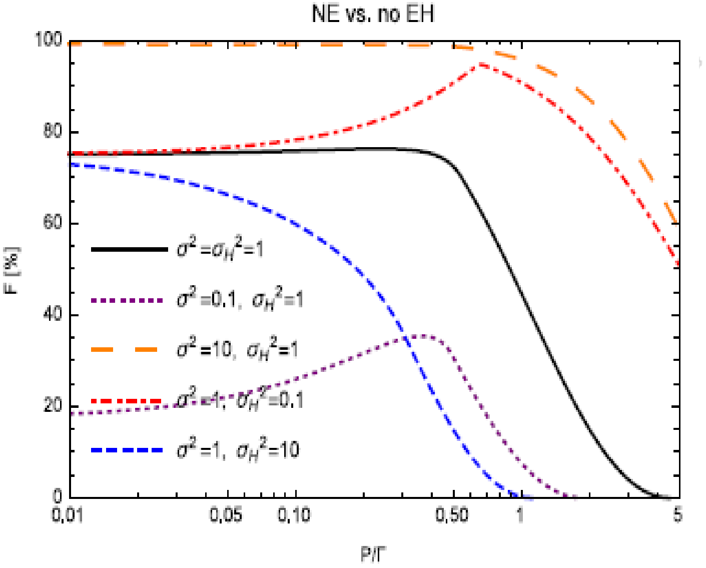


Fig.4. Relative utility gain at the NE vs. no EH: $F = (C^{NE} - C^{noEH})/C^{NE}$ **as a function of** $P/\Gamma \geq 0$ **for** ζ **= 0:7 and different channel parameters.**

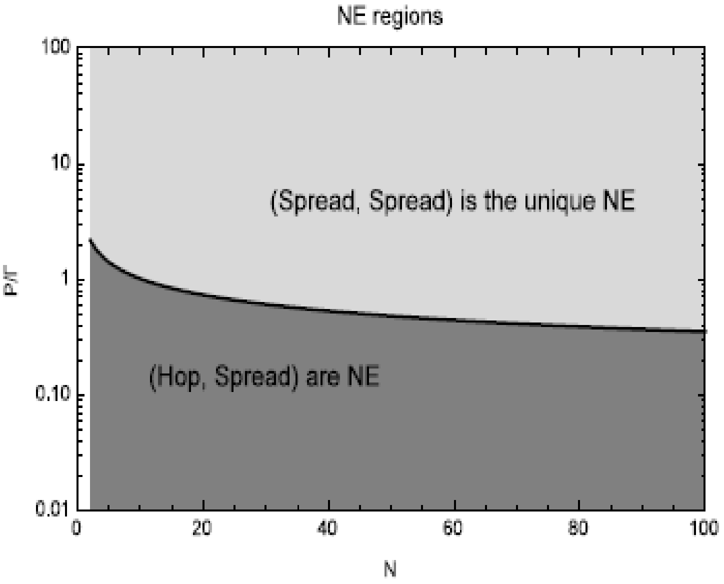


Fig.5. NE regions as a function of $P/\Gamma \geq 0$ **and** $N \geq 2$ **for** $\Gamma = \sigma_A^2 = \sigma_B^2 = \sigma_H^2 = 1$**.**

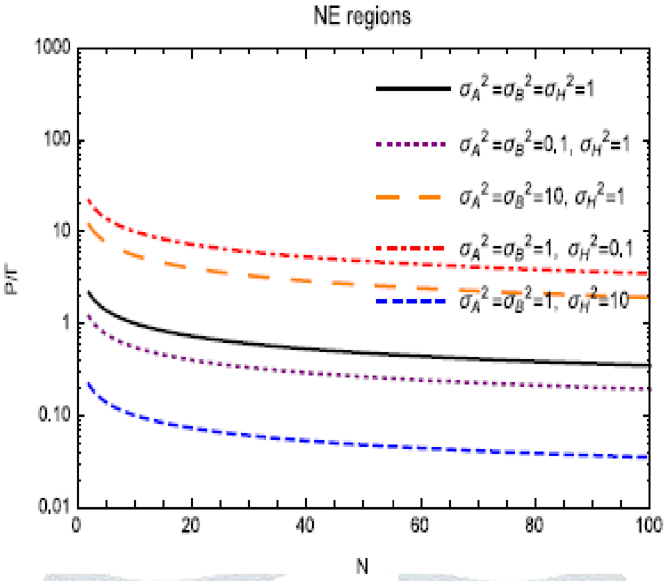


Fig.6. NE regions as a function of $P/\Gamma \geq 0$ and $N \geq 2$ for $\Gamma = 1$ anddifferent channel parameters.

VI. SCREENSHOTS

Screenshots of this paper is as shown in bellow Figs.7 to 24.

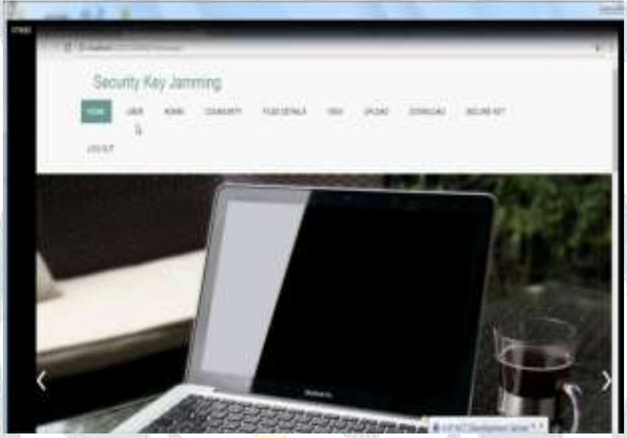


Fig.7. Home Page.

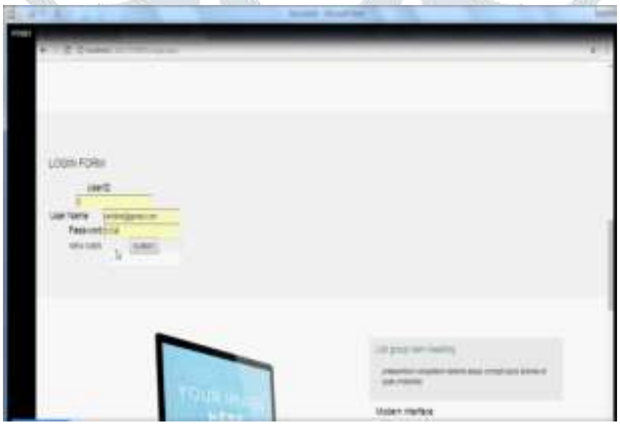


Fig.8. User Login.

PROTECTING SECRET KEY GENERATION SYSTEMS AGAINST JAMMING: ENERGY HARVESTING AND CHANNEL HOPPING APPROACHES

Fig.9. Upload.

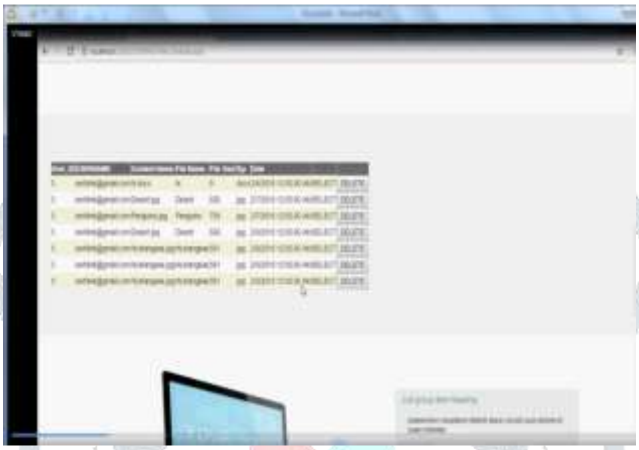


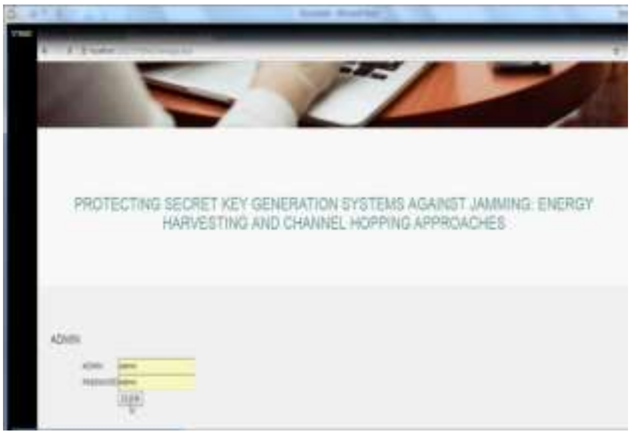
Fig.10. User Files View Details.

Security Key Jamming

Fig.11. Key Generation.

Security Key Jamming

Fig.12. Encryption Key Success.



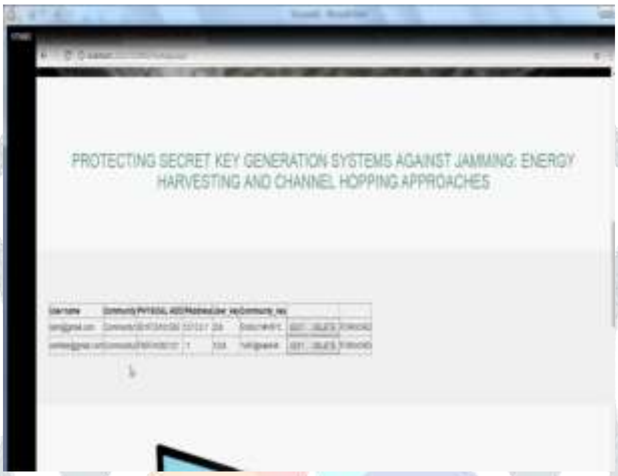
PROTECTING SECRET KEY GENERATION SYSTEMS AGAINST JAMMING: ENERGY HARVESTING AND CHANNEL HOPPING APPROACHES

ADMIN

ADMIN: admin

PASSWORD: admin

Fig.13. Admin.

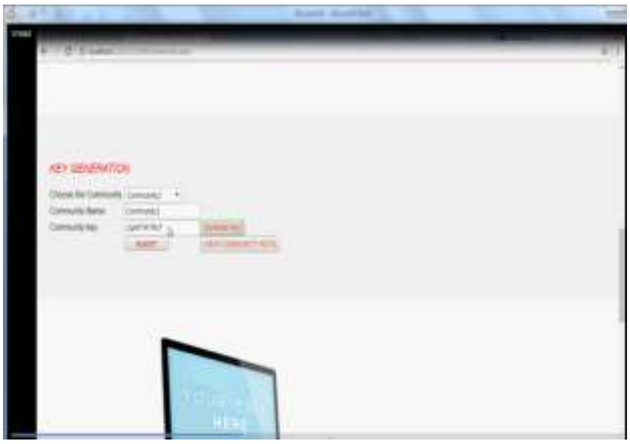


PROTECTING SECRET KEY GENERATION SYSTEMS AGAINST JAMMING: ENERGY HARVESTING AND CHANNEL HOPPING APPROACHES

Fig.14. View Details.

Security Key Jamming

Fig.15. Forwaded Successfully.



KEY GENERATION

Fig.16. Community.

KEY GENERATION

Choose the Community

Community Name

Community key

Fig.17. Key Generation.

Fig.18. Update Key.

Fig.19. Files Details.

PROTECTING SECRET KEY GENERATION SYSTEMS AGAINST JAMMING: ENERGY HARVESTING AND CHANNEL HOPPING APPROACHES

Fig.20. User File Details.

PROTECTING SECRET KEY GENERATION SYSTEMS AGAINST JAMMING: ENERGY HARVESTING AND CHANNEL HOPPING APPROACHES

Community

Fig.21. User Community.

Fig.22. File Details.

Fig.23. Download Files.

Fig.24. Log Out.

VI. CONCLUSION

In this work, the antagonistic communication between a couple of real hubs and a malevolent jammer in a remote mystery key age (SKG) system was explored. Two distinctive counter-sticking methodologies were proposed and considered. To start with, vitality gathering at the authentic hubs, and, second, channel jumping versus control spreading in square blurring AWGN channels. In either approach, a zero-entirety diversion was presented as the targets of the two gatherings included were contradicted. Finish portrayals of the Nash and Stackelberg equilibria in shut frame were given in the two cases. It was exhibited that either approach may offer critical picks up in utility, especially in the low flag tointerference proportion administration, in which balancing the sticking impedance ends up significant. Accordingly, reasonable and low many-sided quality choices for shielding SKG frameworks might be produced by abusing either novel handset highlights or accessible unearthly assets.

VII. REFERENCES

[1] E. Belmega and A. Chorti, “Energy harvesting in secret key generation systems under jamming attacks,” in Proc. IEEE Int. Conf. Commun.(ICC), to appear, May 2017.

[2] A. Chorti and E. Belmega, “Secret key generation in Rayleigh blockfading AWGN channels under jamming attacks,” in Proc. IEEE Int.Conf. Commun.(ICC), to appear, May 2017.

[3] R. Ahlswede and I. Csisz´ar, “Common randomness in information theoryand cryptography – part I: Secret sharing,” IEEE Trans. Inf. Theory,vol. 39, no. 7, pp. 1121–1132, Jul. 1993.

[4] U. Maurer, “Secret key agreement by public discussion based oncommon information,” IEEE Trans. Inf. Theory, vol. 39, no. 5, pp. 733–742, May 1993.

[5] R. Ahlswede and I. Csisz´ar, “Common randomness in information theoryand cryptography – part II: CR capacity,” IEEE Trans. Inf. Theory,vol. 44, no. 1, pp. 225–240, Jan. 1998.

[6] C. Bennett, G. Brassard, C. Cr´epeau, and U. Maurer, “Generalizedprivacy amplification,” IEEE Trans. Inf. Theory, vol. 50, no. 2, pp. 394–400, Feb. 1995.

[7] C. Ye, A. Reznik, and Y. Shah, “Extracting secrecy from jointly Gaussianrandom variables,” in Proc. Int. Symp. Inform. Theory (ISIT), Seatle, US,Jul. 2006, pp. 2593–2597.

[8] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam,“Information-theoretically secret key generation for fading wirelesschannels,” IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 240–154, Jun. 2010.

[9] T.-H. Chou, S. Draper, and A. M. Sayeed, “Key generation using externalsource excitation: Capacity, reliability and secrecy exponent,” IEEETrans. Inf. Theory, vol. 58, no. 4, pp. 2455–2474, Apr. 2012.

[10] W. Yunchuan, Z. Kai, and P. Mohapatra, “Adaptive wireless channelprobing for shared key generation based on PID controller,” IEEE Trans.Mobile Comput., vol. 12, no. 9, pp. 1842–1852, Sep. 2013.
[11] A. Mukherjee, S.A.A., Fakoorian, H. Jing, and A. Swindlehurst, “Principlesof physical layer security in multiuser wireless networks: A survey,”IEEE Commun. Surveys and Tuts., vol. 16, no. 3, pp. 1550–1573, ThirdQuarter 2014.
[12] O. Gungor, F. Chen, and C. Koksal, “Secret key generation via localization and mobility,” IEEE Trans. Veh.Technol., vol. 64, no. 6, pp.2214–2230, Jun. 2015.
[13] U. Maurer and S. Wolf, “Secret-key agreement over unauthenticated public channels-part III: privacy amplification,” IEEE Trans. Inf. Theory,vol. 49, no. 4, pp. 839–851, Apr. 2003.

Author’s Details:

MrMirza Burhan Baig has completed his B.Tech in computer science and engineering from Nawab Shah Alam Khan College Of Engineering And Technology, Hyderabad, TS, JNTU Hyderabad. Presently, he is pursuing his Masters in computer science and engineering from Shadan College Of Engineering And Technology, Hyderabad, TS. India.

Mr Md Ateequr Rahman received his B.E Degree from P.D.A College of Engineering, Gulbarga, Karnataka, India in 2000. In 2004, He obtained M.Tech degree in Computer Science & Engineering from Visvesvaraya Technological University, Hyderabad, India. He is currently pursuing Ph.D. from Jawaharlal Nehru Technological University, Hyderabad, India. Presently he is working as Associate Professor in Computer Science & Engineering Dept, S.C.E.T Hyderabad. His areas of interest include Spatial Databases, Spatial Data Mining, Remote Sensing, Image Processing and Networks protocols etc.