Improving Physical Layer Security Using Hybrid Techniques in Wireless Communication

[1]Dr. Hemant Dhabhai, [2]Mr. Aabhas Mathur, [3]Ritu Kumari Sharma, [4]Mr. Khushal Agrawal

[1]Associate Professor, [2]Associate Professor, [3]M. Tech Scholar, [4]Senior Engineer
[1]Department Electronics & Communication
Aravali Institute of Technical Studies, Umarda, Udaipur (Raj), India
Email - [1]hemant1_anu@rediff.com, [2]aabhas08mathur@gmail.com, [3]ritusharma100892@gmail.com, [4]khushalagarwal20@gmail.com

Abstract: *According to the origination of RF (Radio) spread, remote correspondences can be effectively caught by unapproved clients for capture attempt and along these lines remote correspondence are very powerless against overhang dropping assaults by abuse of physical attributes of remote channels. The propose work is centered around advancement of assorted qualities strategies to improve physical layer security, denoting an outlook change from traditional manufactured clamor era and pillar shaping systems. Manufactured commotion procedures are exceedingly control hungry and require on extra level of energy limit which is not appropriate for better worked framework. In this way work is engaged at improvement of another procedures utilizing variable length cryptography in which MAC (Medium Access Control)/address of the remote hubs for key era purposes. Likewise, it is proposed, that the keys for correspondence encryption are randomized by a worldwide time source, for example, GPS or inward ace RTC (Real Time Clock). This interesting component permits a high level of security as keys are really arbitrary because of Millisecond level synchronization key randomization utilizing a worldwide exact time source office profoundly secure correspondence in a shut gathering. Additionally, the creator has proposed key expiry time, after slip by station of such time, all key should be sham completely recovered.*

Key Words: *Physical Layer, Security, RF Propagation, Wireless Network, Random Key Generation, Mixed Key Cryptography, GPS clock.*

1. INTRODUCTION:

In remote frameworks, the transmission between veritable customers can be adequately gotten by an eavesdropper for catch endeavor as a result of the impart method for remote medium, making the remote transmission significantly exposed against tuning in strikes. Remembering the true objective to fulfill the private transmission, existing correspondences structures consistently get the cryptographic techniques to shield a rubberneck from tapping the data transmission between genuine customers. By considering the symmetric key encryption for example, the main data (called plaintext) is first encoded at source center point by using an encryption figuring close by a riddle key that is granted to objective center point in a manner of speaking. By then, the mixed plaintext (generally called figure content) is transmitted to objective that will unscramble its got figure content with the pre-shared secret key. Thus, paying little heed to the likelihood that a busybody gets the cipher text transmission, it is up til now difficult to decipher the plaintext by the spy from its got cipher text without the secret key. It is pointed out that the cipher text transmission is not faultlessly secure, since the cipher text can regardless be decoded by a meddler with the intensive key request, which is generally called the creature drive attack. To this end, physical-layer security is creating as an alternative perspective to guarantee the remote trades against listening stealthily attacks, including the monster compel ambush Physical-layer security work was led by Wyner in , where a discrete memoryless wiretap channel was broke down for secure correspondences inside seeing an eavesdropper. It was shown in that the radiantly secure data transmission can be proficient if the channel furthest reaches of the principal association (from source to objective) is higher than that of the wiretap interface (from source to spy). Later on, in, the Wyner's results were connected from the discrete memoryless wiretap channel to the Gaussian wiretap channel, where an assumed secret breaking point was made and showed up as the refinement between the channel furthest reaches of the standard associate and that of the wiretap interface. In case as far as possible falls underneath zero, the transmission from source to objective winds up observably flimsy and the spy would win with respect to catching the source transmission, i.e., a square event happens. With a particular true objective to upgrade the transmission security against listening stealthily strikes, it is of centrality to decrease the probability of occasion of a catch event (called piece probability) through enlarging as far as possible. Nevertheless, in remote correspondences, as far as possible genuinely corrupts in view of the obscuring sway. [4] [5] [6]

2. LITERATURE REVIEW:

Because of the communicate way of radio engendering, the remote transmission can be promptly over heard by unapproved clients for block attempt purposes and is subsequently exceedingly powerless against listening in assaults. To this end, physical-layer security is rising as a promising worldview to ensure the remote correspondences against listening stealthily assaults by misusing the physical qualities of remote channels. This article is centered around the examination of differences strategies to enhance the physical layer security, varying from the regular artificial clamor era and pillar framing procedures which normally devour extra power for creating artificial commotion and display high usage many-sided quality for shaft previous outline. We exhibit a few differing qualities ways to deal with enhance the remote physical-layer security, including the numerous information various yield (MIMO), multi client assorted qualities, and helpful differences. To represent the security change through differing qualities, we propose a contextual investigation of misusing agreeable transfers to help the flag transmission from source to goal while safeguarding against listening stealthily assaults. We assess the security execution of agreeable hand-off transmission in Rayleigh blurring situations as far as mystery limit and catch likelihood. It is demonstrated that as the quantity of transfers expands, the mystery limit and block likelihood of the agreeable hand-off transmission both enhance significantly, inferring the benefit of abusing helpful differing qualities to enhance the physical-layer security against listening stealthily attacks.[1] [2] [3]

3. METHODOLOGY:

Key Randomization Utilizing Time Synchronization

While information is transmitted between trusted capable hubs, the noxious hubs can think about the whole transmission. To escape all sort of burglary, a random key is generated. This random key is generated by generating any random number. Now this random number is not only the solution to secure the data since it is a irregular key. This irregular key can be more secure if we further randomize it by doing XOR with GPS/Atomic clock and hence we get a truly random key thereby making our system more secured. Since GPS provides different time at different instants and thus creating different truly random keys at instants of time.

$$\text{Truly Random Key} = \text{Random Key} \oplus \text{GPS / Atomic Clock}$$

Fig.3.1 Truly Random Key Using GPS/Atomic Clock

Limit Time Key Expiry

For this situation, the irregular key naturally change at the fix time Cycle. Since the administrator would prefer not to tell anybody about the genuinely irregular key so that the really arbitrary key changes or resets after predefined time. For Instance, on the off chance we kept the reset time as 30 seconds in key server, than it would consequently change after every 30 seconds and it will take the time from GPS clock and will be randomized and after every 30 seconds the new truly random key will be generated. This 30 seconds time is known as limit time key expiry. It is the main key factor involved in this research area as after this expiry time a new key will be generated by randomizing the value with the time taken by GPS clock which will always give a different value and thereby obtaining different truly random keys after different instants of time.

Cutoff Time Key Expiry

For this circumstance, the sporadic key normally changes at the fix time Cycle. Since the overseer would lean toward not to be enlightened anyone concerning the really unpredictable key. So that, the truly self-assertive key relentless change or reset at a settled time. For Instance, in case we kept the reset time of advance 30 second in key server, than it thusly change into another subjective key. [9]

Separation Amongst Hubs and Beneficiary power

This is also a feature additional to key randomization. This feature can be added to an area depending on the distance between the key server and the trusted hubs. Here we can set a maximum and minimum value of power reception from the hubs to the key server. Received power is a function of distance which is inversely proportional to each other. If the distance between the key server and the trusted hub is closest then we get maximum power and if the distance between the key server and the trusted hub is farthest then we get a minimum power.

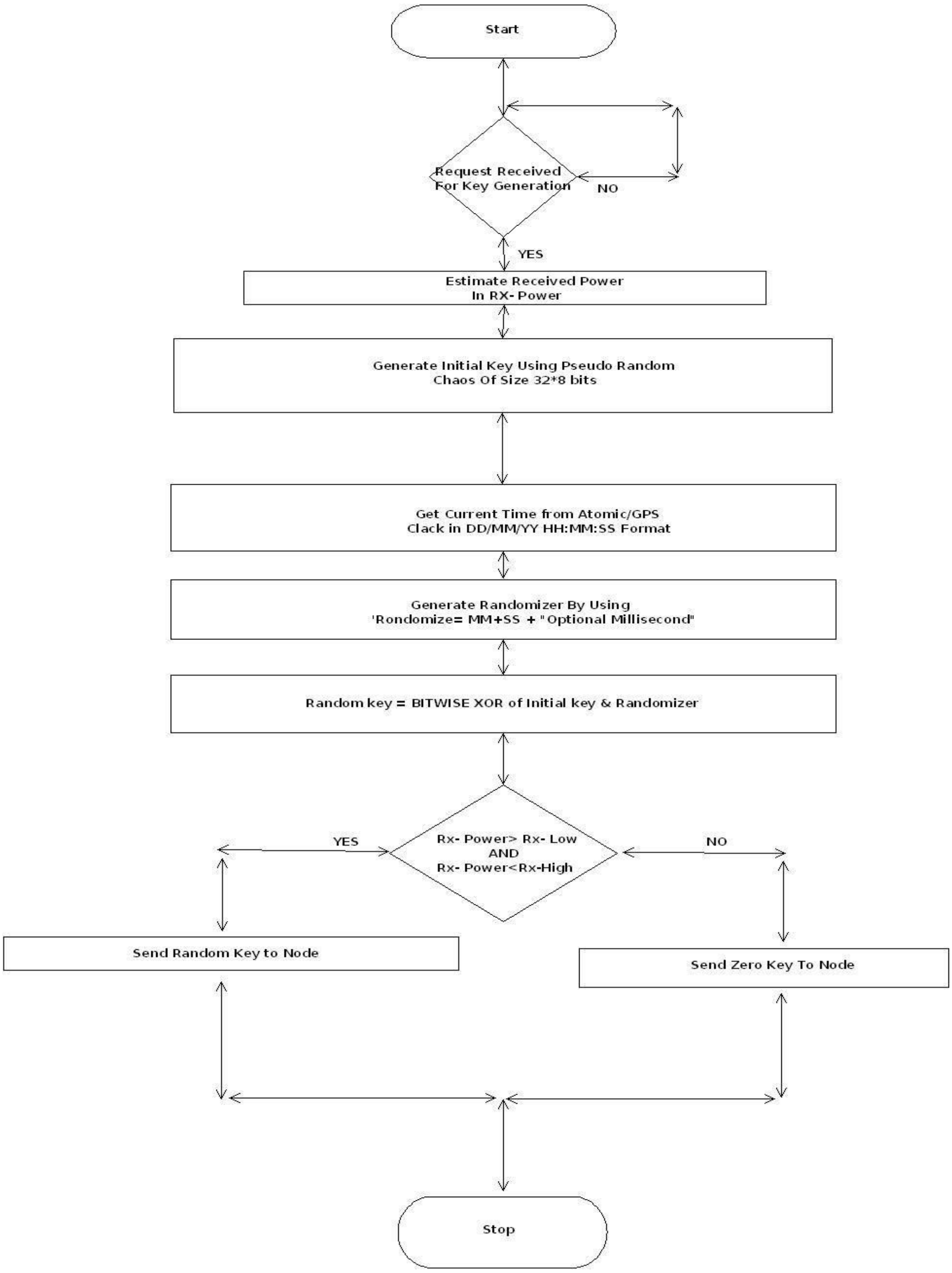
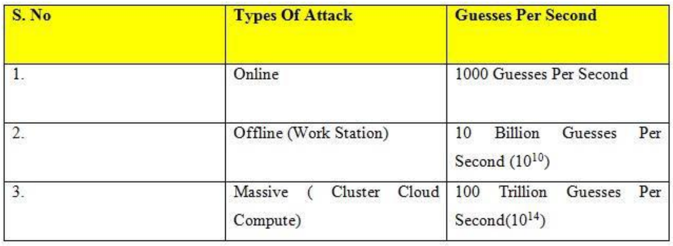

Start
Request Received
For Key Generation
NO
YES
Estimate Received Power
In RX- Power
Generate Initial Key Using Pseudo Random
Chaos Of Size 32*8 bits
Get Current Time from Atomic/GPS
Clack in DD/MM/YY HH:MM:SS Format
Generate Randomizer By Using
'Rondomize= MM+SS + "Optional Millisecond"
Random key = BITWISE XOR of Initial key & Randomizer
YES
Rx- Power> Rx- Low
AND
Rx- Power<Rx-High
NO
Send Random Key to Node
Send Zero Key To Node
Stop

Fig.3.1 Flowchart of Truly Random Key Generation Server

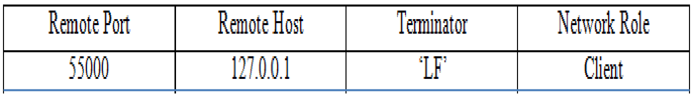
4. RESULTS:

Table 4.1 Guesses per Second



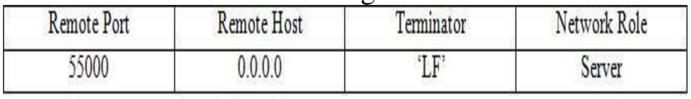
S. No	Types Of Attack	Guesses Per Second
1.	Online	1000 Guesses Per Second
2.	Offline (Work Station)	10 Billion Guesses Per Second (10^{10})
3.	Massive (Cluster Cloud Compute)	100 Trillion Guesses Per Second(10^{14})

Table 4.2 Master Wireless Node Network Characteristics



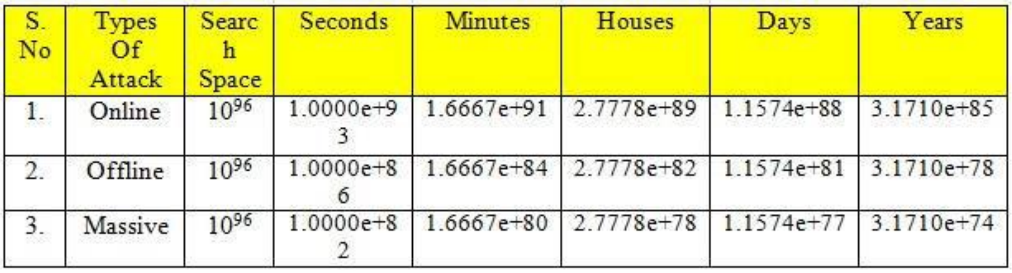
Remote Port	Remote Host	Terminator	Network Role
55000	127.0.0.1	'LF'	Client

Table 4.3 Truly Random Key Server Network Characteristics
5tv g



Remote Port	Remote Host	Terminator	Network Role
55000	0.0.0.0	'LF'	Server

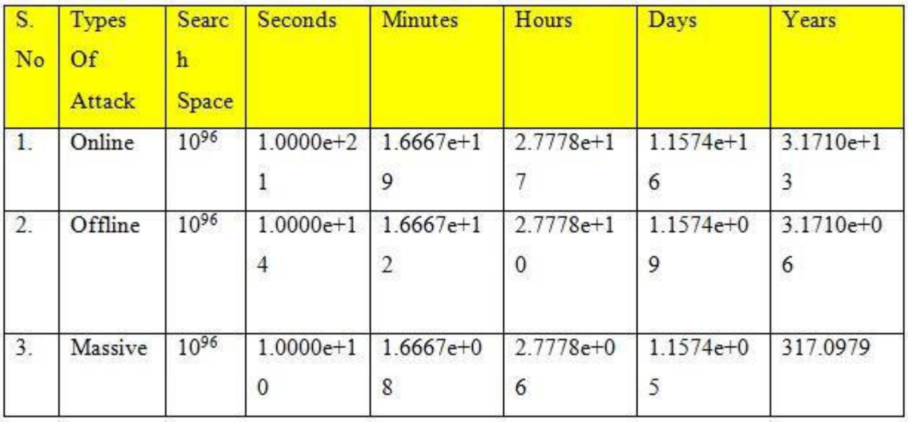
Table 4.4 100% Key Recovers



S. No	Types Of Attack	Search Space	Seconds	Minutes	Houses	Days	Years
1.	Online	10^{96}	1.0000e+93	1.6667e+91	2.7778e+89	1.1574e+88	3.1710e+85
2.	Offline	10^{96}	1.0000e+86	1.6667e+84	2.7778e+82	1.1574e+81	3.1710e+78
3.	Massive	10^{96}	1.0000e+82	1.6667e+80	2.7778e+78	1.1574e+77	3.1710e+74

When, we are applied the different types of attack then we set up 32 values and 3 digits and total of 96 digits and we taken 100% key recover after the taken values defined the online brute force attack and first measuring for seconds and total guesses password is divided from the total search space and multiply from total second of the day. Output result is coming in 85 years estimated which mean that system will recover the key in 3.1710e+85 years and others two methods are which is offline and massive attack is already taken 78 and 74 years approximately.

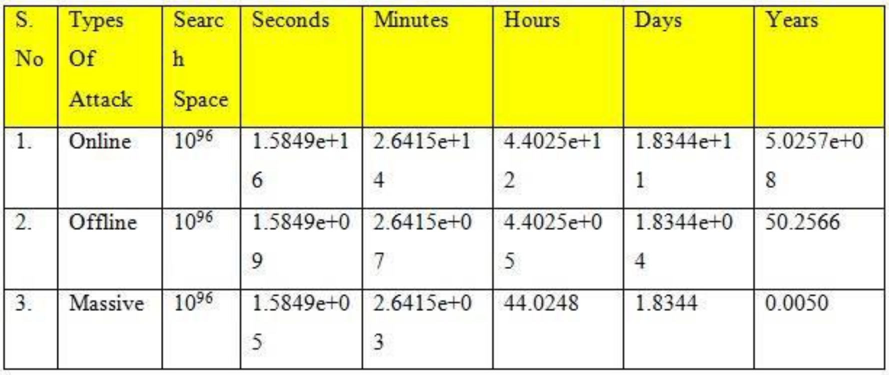
Table 4.5 25% Key Recovers



S. No	Types Of Attack	Search Space	Seconds	Minutes	Hours	Days	Years
1.	Online	10^{96}	1.0000e+21	1.6667e+19	2.7778e+17	1.1574e+16	3.1710e+13
2.	Offline	10^{96}	1.0000e+14	1.6667e+12	2.7778e+10	1.1574e+09	3.1710e+06
3.	Massive	10^{96}	1.0000e+10	1.6667e+08	2.7778e+06	1.1574e+05	317.0979

When, the brute force time computation for 25 percentage key recover then time will decrease 13 years for online attack and 06 and 09 years for offline and massive attacks.

Table 4.6 20% Key Recovers



S. No	Types Of Attack	Search Space	Seconds	Minutes	Hours	Days	Years
1.	Online	10^{96}	1.5849e+16	2.6415e+14	4.4025e+12	1.8344e+11	5.0257e+08
2.	Offline	10^{96}	1.5849e+09	2.6415e+07	4.4025e+05	1.8344e+04	50.2566
3.	Massive	10^{96}	1.5849e+05	2.6415e+03	44.0248	1.8344	0.0050

When, brute force attack time computation for 20% key recover then then time will rapidaly deacrease for online attack it will be 8 years and for offline attck it will be 0.2 years and for massive attck is 0.005 years. For example,

It mean that it will attack within 13 minitus cycle, so we could changed the password and recover within 8 minitus cycle so the possibility of attacking will be infinity.

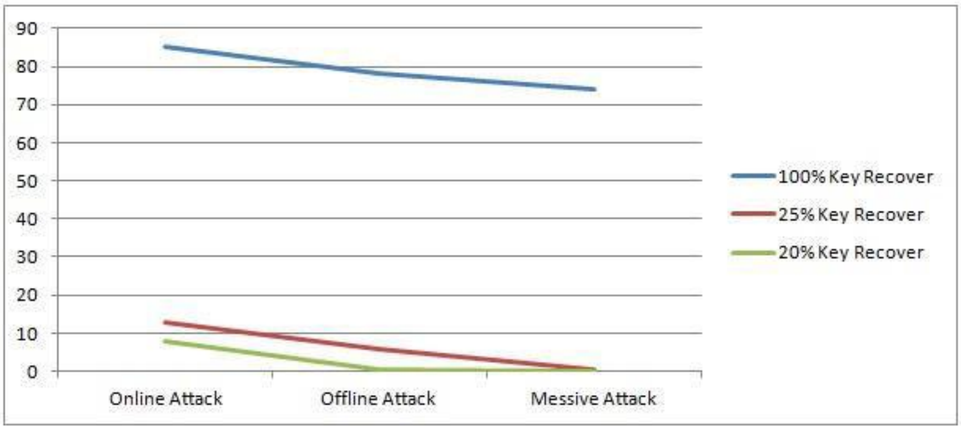


Fig. 4.1 Graphs Between 100% And 25%, 20% Key Recover

5. CONCLUSION:

This work is away for examination of physical layer security of remote correspondence and showed a couple in headway varying qualities methods for upgrading the remote security against listening stealthily and catch endeavor strikes. The maker has made cross breed frameworks to upgrade physical layer security of remote framework by using sporadic key, discretionary length cryptography in conjunction with Macintosh address or machine address of working centers. Furthermore the maker has displayed a high security standard by synchronization of encryption/unraveling key with an exceedingly correct overall time source. Moreover, normally recuperating key after a predefined the timetable time future mistakes the issue for the eavesdropper and along these lines self-assertive us with a high secure remote framework. The proposed structure in this way been affirmed by exploratory result in this manner maker can suit a reasonable system that can be organize on the present structure.

REFERENCES:

1. Yulong Zou, Jia Zhu, Xianbin Wang, and Victor C.M. Leung, "Improving Physical-Layer Security in Wireless Communications Using Diversity Techniques" IEEE , May 2014.
2. H. Vincent Poora, Rafael F. Schaeferb , "Wireless physical layer security" , PNAS ,vol. 114 , no. 1, pp. 19–26, January 3, 2017.
3. Kyusung Shim , Nhu Tri Do , Beongku A ,"Performance Analysis of Physical Layer Security of Opportunistic Scheduling in Multiuser Multirelay Cooperative Networks", Sensors 2017, 17, 377.
4. Lukman A. Olawoyin , Munzali A. Abana, Yue Wu, Hongwen Yang "A Two-Hop Multi-Relay Secure Transmission with Improved Suboptimal Relay Selection Scheme" , Journal of Communications Vol. 11, No. 6, June 2016.
5. Qian Yu Liau, Chee Yen Leow, and Zhiguo Ding "Physical Layer Security Using Two-Path Successive Relaying", Sensors 2016, 16, 846.
6. Xiaoming Chen, Caijun Zhong, Chau Yuen, and Hsiao-Hwa Chen, "Multi-Antenna Relay Aided Wireless Physical Layer Security" , IEEE Communications Magazine, Feature Topic On Wireless Physical Layer Security, June 2015.
7. Kanapathippillai Cumanan, Hong Xing, Peng Xu, Gan Zheng, Xuchu Dai, Arumugam Nallanathan, Zhiguo Ding and George K. Karagiannidis , "Physical Layer Security Jamming: Theoretical Limits and Practical Designs in Wireless Networks" , IEEE.
8. S.Niranjani, R.Nirmalan, "Wireless Communication Security Through Symbol Obfuscation in Physical Layer" International Research Journal Of Engineering And Technology (Irjet), vol. 02 Issue. 08, pp. 898-900, Nov-2015.
9. Yulong Zou, Jia Zhu, Xuelong Li, and Lajos Hanzo, "Relay Selection for Wireless Communications Against Eavesdropping: A Security-Reliability Tradeoff Perspective", IEEE Network Magazine, September 3, 2015.