# Shadowing Model For Secret Key Extraction From WSN

**Shekhar M. Nalawade**
Computer Engg. Dept., Sinhgad Institute of Technology
Lonavala, S.P.P.U, Pune, India
Email:  nalawade_shekhar@yahoo.co.in

**Sachin D. Babar**
Computer Engg. Dept., Sinhgad Institute of Technology
Lonavala, S.P.P.U, Pune, India
Email:sdbabar@gmail.com

***Abstract*—We propose a new solution for key generation process on the basis of Received Signal Strength (RSS) for wireless sensor nodes. We use simulation environments to show that RSS at both the communicating parties is same due to high data transmission rates is a random characteristic and can be used to generate a secret key. We also try to show that how it can become vulnerable if proper care is not taken about the architecture of system.**

**Few solutions were which were provided for the key generation like its pre-distribution and other key generation algorithms results in repetition of keys after particular interval. Pre-distribution means that provider has to imprint the legitimate key on product itself but such keys results in unreliable to end users. In our architecture design our key generation basis itself is different so it automatically will be helpful for us to design random secret key. Mathematical calculation capabilities of wireless senor nodes are limited so it's unavoidable to use some adversary which will do calculations on behalf of them and provide a key.**

**It's well known to everyone now that random secret key generation and its authentic distribution will be an important characteristic of wireless networks.  After we complete the generation of key we should be use very secured mechanism so that key can be distributed among wireless sensor nodes. Finally we show that, how RSS calculations are random as per the position of nodes in the network and how we have achieved so.**

***Keywords—Received Signal Strength, ZigBee Sensor Nodes, Shadowing Model, 802.15.4, Shadowing Model***

## I. Introduction (*Heading 1*)

Wireless Sensor Nodes are resource constrained devices, so using them for various tasks introduces few more devices specifically to handle infrastructure activities. To establish a secure and authentic connection we require random cryptographic keys which have to be a pioneer characteristic of key generation algorithm.

Requirement of secure data communication in wireless environment has become basic feature of key and security algorithms. Some solutions were designed very basic in nature like pre-deployment of keys on devices itself. But why one should believe on pre-calculated data by manufacturer. Here trust becomes an important factor between the two parties. So eventually it fails to be authentic. Also in WiFi networks has shown that useless security fails to protect the environment access and eventually end up in possible vulnerability. As well as unaware users of WiFi network where users don't configure it properly can easily give up and have their own network unprotected.

Because of all these reasons we have considered the alternatives as follows

- Designing keys on timely basis.
- And send those keys clearly over radio channel.

Key feature which makes a successful key generation algorithm is, it should be a good random number generator so that vulnerability of same reduces to great extent.

In this paper, we trying to show that how RSS can be used as source for random number generator and eventually to design a various secret keys for secure communication which is our final goal. The results show that due to constant bit rate (CBR) we have synchronized transmission.

User has to place three mobile devices on surface of size 1000 x 1000 sq.ft under shadowing model specifications. Initially one device starts communication with another at particular time intervals we calculate the RSS and we record it. After some time third mobile device starts communicating with second device and we do same kind of record keeping of RSS values. Remember that we are doing one-way communication in both the ways and just trying to show even there is common party being communicated results are different due to location differences.

Reason to chose a shadowing model is that it overcomes two major disadvantages each of a Two-ray ground propagation and free space model as follows:-

| Sr. No. | Propogation Model | Disadvantage |
|---|---|---|
| 1 | Free Space Model | 1. One clear line of Sight<br>2. Communication range as a circle |
| 2 | Two-ray Propagation Model | 1. Poor results for short distances<br>2. Communication range as a circle |

Finally we show that RSS calculations are varying between nodes and can be used as source for random number generator algorithm. No extra infrastructure is introduced to store and calculate the secret key.

Remaining paper is organized as Literature survey on section II, Architecture and problem formulation in section III. Section IV, V consists of Mathematical Model, Simulation Scenario respectively. Moreover, last the conclusion & Future scope and References on section VI and VII respectively.

## II. Literature Survey

Methodologies proposed in [1] tries to overcome the problems in public key cryptosystem( PKC) and uses the approach of defining the characteristics of an UHF channel and uses mutual information as a cryptographic variable. It had also discussed the bandwidth as a protection medium and discusses how channel characteristics can be used for creating cryptographic variable. Our discussion in [1] is finally well synthesized by introducing the trapdoor deconvolution which gives us capability to know whether how decryption is possible.

What care we need to take while its fading channel is well formed in [2] with help of random number generator and HASH function on frames basis. This complete process in then analyzed with the help of calculating the probability of protocol failure cases by using formulation for the same. At the end of [1], shows the results which are categorized on the basis of different configuration and parameters which shows that how much stable key can be generated.

By studying the characteristics of cryptographies we start the discussion in [3] which is supported by constant bit rate (CBR) assumption which is very much true to great extent. In designed architecture of proposed system in [3],[15] we can see different antennas used so that heterogeneous systems can be addressed and key agreement can be achieved and we do succeed in the same. But at the end the key generation algorithm has to undergo the some criteria's like Key dis-agreement probability (KDP), Quantization to remove errors in common information shared between communicating nodes which is again a basics for the key generation because it works as a basic random number generator(RNG).

Gaussian random variables introduced in [4], helps us the same way but uses Rayleigh or Rician fading's with AWGN noise to enhance the discussion implementation goes through the three step process of quantization, channel code estimation and Log-likelihood ratio computation in which Bob uses the modified belief-propagation algorithm. To do same Bob has to calculate the log-likelihood ratio (LLR). Performance evaluation in [4] is supported with the parameters like secrecy rates mode wise which gives us better idea about how better particular coding used is.

Lower layer enforcements evolved in [5] lead us to new thinking of securing the lower layers which causes control variations in common information shared between communicating users which is used as random number generator. Here we mainly focus on providing confidentiality and authentication through physical layer security. In process of communication bob receives a convolution signal from Alice in combination with channel response and receiver side noise. Physical layer based authentication goes through the variant discussion like channel based authentication, maintenance of channel authenticator. Also to enhance the physical layer based confidentiality we cover the how channel estimates will be used for key extraction, key dissemination via channel state masking and key dissemination via probabilistic encoding. All this at end is supported by experimental setup and evaluation of performance criteria's.

Principle of reciprocity is basic assumption made in [1]-[6], which give us capability to say that mutual information shared same time stamp is most likely to be equal even in presence of noise over a communication channel. We know that wireless channels are always non-stationary which can used to achieve enough entropy in secret keys and fading graphs can be used to generate secret keys. Deep fades are actually the deviation or attenuation which has affected the signal characteristics over medium of propagation; same is use as RNG in [6]. Threshold mechanism which will eventually design a secret key from the proposed RNG is shared very well mathematically. To support the principle of reciprocity channel coherence time is used as supportive characteristic which will give mutual information as a same. After that key generation is proposed on basis of two mechanisms as key verification information and fuzzy information reconcilliator's.

Study of UWB channels is well characterized in [7], [8], [10] which will take us to the new heights of understanding the similarity of mutual information. For that what they did is they considered the single-path, multipath and UWB link budget, mobility and bandwidth as criteria's as channel characterizing terms. After considering these terms to model the UWB channels we evaluate secret sharing with communication rate constraint and discuss public communication methods to let us know how different algorithms can be result for secret sharing.

For doing study of ITU channels [8], we characterize them with the help of reciprocity nature even in presence of deep fades and SINR. In [8] we use jointly Gaussian random variables to generate the secret key by considering multipath fading channel model [8], [9]. After that we move towards binding the upper bound on secret key rates.

Multipath communication [9] is again discussed for secret key generation with the very support of physical layer modeling and performance evaluation on the basis of independence, secret key for common link and energy consumption for secret key calculation.

Four step approach of key generation for UWB channels is more deep thinking of secret key generation [10] , which says that first we do randomness sharing then information reconciliation supported by privacy amplification with last step as a secure communication. To support the approach they have proposed the channel modeling which is characterized by probability distribution of k-th tap of channel. They have considered RMS delay spread, Power decay profile and Number of multipath components as features of UWB channels. Path modeling is done for single and multipath also [10]. Simulation is performed with IEEE 802.15 standard so that theory channel model and simulated channel results can be compared well.

Till this point we have seen how keys can generated in various authentic channels [1-10] , but when we see the unauthentic channel our considerations changes in various aspects. Our new approach says that first convert theoretic ideas into practical protocol then design a new algorithm whose basic consideration is that we don't have authentic channels for communication. At last we have to validate the impulse responses measures using IEEE 802.11 standard [11]. To support the same after considering key generation aspects they have given a thought to possible attacks that can be made to proposed system like preventing spoofing attacks so that mutual information shared can't be violated. To perform the same action they modify the proposed algorithm and device a new one.

Principle of reciprocity can also be used as an application of detection unauthorized access of wireless access [12]. The challenge in securing the access was that managing and verifying the digital certificates, signal strength as criteria for the selection of new AP and it was very easy to set up a fake AP. Using IEEE 802.11 standard and with the support of linear programming method and least-square fitting methodology they propose a new algorithm to detect fake AP's.

Principle of reciprocity is also questioned as it might not stand in few cases where channel is unauthenticated or shared secret key from channel measurements is to be made. To make sure everything goes smooth they have introduced fractional interpolation filtering and then de-correlation transformation is applied followed by multi-bit adaptive quantization to remove errors. Later on MAQ is discussed over probability of disagreement and Gaussian case to approve performance of proposed strategy.

Data communication basics like traffic types handled, architecture of ZigBee, its frame structure, types channel accessing and addressing for same, security measures are described in [14].

By using CBR and principle of reciprocity they have proposed a system where adversary model takes care of creating key for Alice and Bob. Same system has undergone through various comparisons per packet basis to strengthen the considerations made.

In [16] they have considered basics as a channel randomness, independent channel variation over space, channel reciprocity for their proposed system. The same system then passes through various performance parameters like key dis-agreement probability, secret key generation rate. Newly considered performance measures like scalability and implementation issues ads realness to the discussion made.

Phase information not so suitable for secret key generation because of accurateness and implementation issues of same [17]. So they propose the new consideration of reciprocal channel with time division duplex system. This system uses CQG protocol to generate a secret keys and RPA protocol to remove errors. This in-turn may increase the complexity of key generation but increases the reliability and reduces the BER of the system.

Although phase information is not so reliable [17], same is been used as platform by [18] for secret key generation. They have considered the time-slotted roundtrip secret key generation protocol which discusses pairwise key generation and group key generation to address the scalability of proposed algorithm. Also probability of successful secret key generation, bit generation rate, randomness of generated bits are put forth for evaluation.

Using signal strength as channel characteristic and fundamental of secret bit generation is induced [19], which says that even adversary can listen nonce between communicating entities can't generate the same key as they had generated. By using this feature new system is proposed to say that, let there be an adversary in wireless sensor network for random number generation calculation he can't implement the man-in-middle attack even he wants to.

## III. ARCHITECTURAL DESIGN

Here we have three mobile nodes communicating with each other names as Node1, Node2, and Node3. The traditional "Diffie-Hellman" key establishment protocol are  comparable by establishing core in the way of assuming that eavesdropper will not be able to perform a man-in-middle attack at the time of establishment of own key with sensor nodes Node1 and Node2. It aim towards achieving a efficient key distribution in wireless networking at following features

- Low Cost.
- Low Data Rate.
- Low Consumption Power.

Which are the same properties who makes them used worldwide and in various applications.

A four step methodology has been introduces previously to establish a secure communication over a wireless channel.

Step1:- Share the randomness.
Step2:- Information Reconciliation.
Step3:- Privacy Amplification.
Step4:- Establish a secure Communication.

Our primary aim here is that showing that randomness is available and it's best available in shadowing model. Reason for that is tabulated below.

| Sr. No | Characteristic | Enhancement Provided |
|---|---|---|
| 1 | Path-Loss | More accurate RSS calculation |
| 2 | Communication range | Depends on specification of nodes itself, no particular design |
| 3 | Gaussian Random Variable | Greater randomness in RSS value |
| 4 | Nodes Specifications | Can be given manually or dynamically for better practical and ideal scenario results |

Separate event simulators are provided in both wired and wireless network so that routing, TCP simulations and multicast protocols can be handled properly. In 802.15.4 MAC is helpful to implement all 35 MAC sub-layer primitives and 802.14.5 PHY standard is useful to implement all 14 PHY primitives. Features like, Mode of super-frame structure,error link model, queue interface, radio propagation model, radio transmission range, failure in node and link, antenna model and traffic patterns are supported by using animation configuration and guiding light.

## IV. MATHEMATICAL APPROACH

### A. Simulation Environment in NS2

With the help of CBR, UDP (User Datagram Protocol) with AODP routing protocol shows the characteristics of one way and unreliable transmission, packet size, and interval. For providing mare accurate result than free-space and Two-ray grong propagation model, we use shadowing model, at the time of long distance between transmitter and receiver.

Shadowing model in divided in two parts.

1. Path Loss Model
2. Variation of Received power at certain distance

First part is used to predict the mean received power at distance d, which is denoted by $P_r(d)\#$. $P_r(d)\#$ is computed with the help of $P_r(d_0)$. Where $P_r(d_0)$ is known as close-in distance which is used as reference. $P_r(d)\#$ is evaluated as follows

$P_r(d_0) / P_r(d)\# = (d / d_0)^{\beta}$

Where,

β → Path Loss Exponent

β is empirically determined by field measurements. Following table enlists some typical values path loss exponent known.

| Environment | | B |
|---|---|---|
| Outdoor | Free Space | 2 |
| | Shadowed Urban Area | 2.7 to 5 |
| In Building | Line-of-sight | 1.6 to 1.8 |
| | Obstructed | 4 to 6 |

From above table we can conclude that larger values of β corresponds to more obstruction to the signal so we get faster reduction in average received power as distance becomes larger. $P_r(d_0)$ can be calculated using following equation

$P_r(d) = (P_tG_tG_rh_t^2h_r^2)/ (d^4L)$

Here, $P_t$ →signal power transmitter
$G_r$ →antenna gain receiver
$G_t$→antenna gain transmitter
$h_t$→ transmitter antenna height
$h_r$→receiver antenna height

System loss is L (L ≥ 1). $P_r$ the received power signal used as source randomness. Lets assume that, L=1 and $G_t$=$G_r$=1 in an NS2 simulator.

Path loss is usually measured in dB, so from above equation we can say that,

$[P_r(d)\# / P_r(d_0)]_{dB}= -10\beta\log(d / d_0)$

Second part of shadowing model tells us about variation in average received power at certain distance. It's a log-normal random variable i.e.

Gaussian distribution if measured in dB. To represent shadowing model we use following equation

$[P_r(d) / P_r(d_0)]_{dB} = -10\beta\log(d / d0) + X_{dB}$

Where

$X_{dB}$ → Gaussian random variable with zero mean and standard deviation $\sigma_{dB}$ which is known as shadowing deviation calculated by measurement. Some measurements values are enlisted in following table.

| Environment | $\sigma_{dB}$ |
|---|---|
| Outdoor | 4 to 12 |
| Office, Hard partition | 7 |
| Office, Soft partition | 9.6 |
| Factory, Line-of-sight | 3 to 6 |
| Factory, Obstructed | 6.8 |

To summarize we can say that shadowing model extends restriction like ideal circle model to richer statistic model where nodes can only communicate when near the edge of communication range.

B. Simulations Scenario

By using AODV protocol for routing with UDP as a packet care taker we try to show that RSS at different node positions in different as be used as source of randomness. Then its used as an input to secret key generation algorithm, which eventually results in good random number generator.

At the end of simulation we show that even we send packets from between two nodes due CBR we get same RSS values which possible only because of Principle of Reciprocity.

Principle of reciprocity states that if there is an absence of interference both transmitter and receiver will experience same channel characteristics and signal envelopes .

Here we show that even there is interference and other factors which create variations in wireless communication we get same response at both the parties. Also the variation in same is random for random nodes in the architecture.

The variations obtained in RSS can go through various bit stream and information reconciliation processes to generate a secret key. One method is to we define minimum and maximum threshold value. And obtained variation designed graph is sampled for those values and marked as '0' and '1' for minimum and maximum value respectively.

## V. SIMULATION

The NS2 simulations are visualized here. In which we have used shadow propagation model where all three nodes are mobile i.e. Node1, Node2and Node3. Where Node1 and Node2 are communicating with each other and Node1 and Node3 are communicating as a pair. Main feature of this architecture is all the nodes are mobile and can roam anywhere within defined topology boundary of 1000x1000 Sq.ft.

In this simulation nodes even very much nearby to each other but still RSS readings are different. Extra infrastructure can be added in architecture so that secret information after reconciliation process can be used and secret key can be generated.

We will be comparing results on the basis of communication happened between Node1 and Node3, Where we have calculated the RSS values for different co-ordinates. Also we have done same for the Node1 and Node2. At the end we will be compare both the results and prove that how RSS values can be a good random number generators.

Following table will help us to illustrate the same.

| Node 1 | | Node 3 | | RSS Value |
|---|---|---|---|---|
| 1155 | 794 | 1275 | 794 | 1.39028 |
| 1146.06156 | 787.59344 | 1275 | 794 | 1.20124 |
| 1101.35598 | 755.55107 | 1243.79402 | 773.709695 | 9.709886 |
| 1056.65710 | 723.51351 | 1193.44467 | 740.97225 | 1.05282 |
| 1003.013094 | 685.06458 | 1136.94277 | 704.23439 | 1.0937206 |
| 949.3690800 | 646.6156 | 1083.816385 | 669.691312 | 1.0758576 |
| 904.663499 | 614.57329 | 1036.167302 | 638.709603 | 1.119958 |
| 851.019484 | 576.124372 | 982.956884 | 604.111883 | 1.10056673 |
| 806.313903 | 544.082001 | 944.979261 | 579.418614 | 9.777019 |
| 752.669888 | 505.633078 | 878.863383 | 536.429689 | 1.186504 |
| 707.971013 | 473.59551 | 836.838843 | 509.105091 | 1.120457 |
| 654.326998 | 435.1465 | 781.397344 | 473.0567098 | 1.138541 |
| 600.682983 | 396.697667 | 732.014725 | 440.947846 | 1.042385 |
| 547.0389686 | 358.248744 | 669.401371 | 400.236282 | 1.196268 |
| 502.333387 | 326.206373 | 622.513741 | 369.749675 | 1.225274 |
| 448.689372 | 287.757450 | 572.7044732 | 337.363402 | 1.122175 |
| 403.990497 | 255.719886 | 527.160642 | 307.750541 | 1.119816 |
| 350.346482 | 217.270963 | 477.003402 | 275.138014 | 1.032469 |

| | | | | |
|---|---|---|---|---|
| 305.640901 | 185.228592 | 417.583045 | 236.502556 | 1.320585 |
| 251.9968869 | 146.779669 | 370.460997 | 205.863529 | 1.1424004 |
| 207.291306 | 114.737298 | 325.326093 | 176.516554 | 1.127967331 |
| 153.647291 | 76.288375 | 264.169324 | 136.752071 | 1.261432 |
| 108.948415 | 44.250810 | 218.339893 | 106.953511 | 1.259278 |
| 50 | 2 | 156.511713 | 66.7524719 | 1.288495 |
| 50 | 2 | 94.698577 | 26.561214 | 7.696463 |
| 50 | 2 | 60 | 4 | 1.925015 |

Table 1: Movement of sensor Node1 and Node3 and Their RSS values

Also same results are seen for the communication between Node3 and Node1 which results in same RSS values. All this can be seen by comparing following table with Table 1.

| Node 3 | | Node 1 | | RSS Value |
|---|---|---|---|---|
| 1275 | 794 | 1155 | 794 | 1.390289 |
| 1275 | 794 | 1146.061566 | 787.593448 | 1.201246 |
| 1243.794025 | 773.709695 | 1101.355985 | 755.551077 | 9.7098866 |
| 1193.444671 | 740.972255 | 1056.657109 | 723.513512 | 1.0528260 |
| 1136.942778 | 704.234399 | 1003.013094 | 685.0645892 | 1.0937206 |
| 1083.816385 | 669.691312 | 949.36908003 | 646.615666 | 1.0758576 |
| 1036.167302 | 638.7096039 | 904.663499 | 614.573295 | 1.1199584 |
| 982.956884 | 604.111883 | 851.019484 | 576.124372 | 1.1005667 |
| 944.979261 | 579.418614 | 806.313903 | 544.0820013 | 9.77701923 |
| 878.863383 | 536.429689 | 752.669888 | 505.6330784 | 1.18650465 |
| 836.838843 | 509.105091 | 707.971013 | 473.595513 | 1.120457 |
| 781.397344 | 473.056709 | 654.326998 | 435.146590 | 1.13854119 |
| 732.014725 | 440.947846 | 600.682983 | 396.697667 | 1.042385 |
| 669.401371 | 400.236282 | 547.038968 | 358.248744 | 1.19626855 |
| 622.51Litera3741 | 369.749675 | 502.333387 | 326.206373 | 1.22527408 |
| 572.704473 | 337.363402 | 448.689372 | 287.757450 | 1.12217541 |
| 527.160642 | 307.750541 | 403.9904 | 255.719886 | 1.11981668 |
| 477.003402 | 275.138014 | 350.3464 | 217.270963 | 1.03246910 |
| 417.583045 | 236.502556 | 305.64090 | 185.22859 | 1.32058590 |
| 370.460997 | 205.863529 | 251.996886 | 146.779669 | 1.14240042 |
| 325.326093 | 176.516554 | 207.291306 | 114.737298 | 1.12796733 |
| 264.169324 | 136.752071 | 153.647291 | 76.2883751 | 1.26143233 |
| 218.339893 | 106.953511 | 108.948415 | 44.2508101 | 1.25927847 |
| 156.511713 | 66.7524719 | 50 | 2 | 1.28849563 |
| 94.6985772 | 26.5612148 | 50 | 2 | 7.69646381 |
| 60 | 4 | 50 | 2 | 1.92501590 |

Table 2: Movement of sensor Node3 and Node1 and Their RSS values

From Table 1 and Table 2 we can observe that same RSS values are there for same node positions.

Only this observation won't result in good conclusion because the variation is RSS values is been seen till this point. What we should see now is difference between the values for different node positions. This can be shown by looking at following tables Table 2 and Table 3.

| Node 2 | | Node 1 | | RSS Values |
|---|---|---|---|---|
| x | y | x | y | |
| 1022 | 674 | 1155 | 794 | 6.2389 |
| 1022 | 674 | 1137.1 | 781.19 | 8.0915 |
| 1006.7 | 663.75 | 1110.3 | 761.96 | 9.8261 |
| 957.09 | 630.47 | 1065.6 | 729.92 | 9.2409 |
| 908.78 | 598.07 | 1012 | 691.47 | 1.0336 |
| 841.33 | 552.83 | 958.31 | 653.02 | 8.44 |
| 807.42 | 530.09 | 922.55 | 627.39 | 8.811 |
| 759.4 | 497.89 | 868.9 | 588.94 | 9.8709 |
| 707.8 | 463.28 | 824.2 | 556.9 | 8.9724 |
| 648.99 | 423.84 | 770.55 | 518.45 | 8.4373 |
| 602.88 | 392.91 | 725.85 | 486.41 | 8.3896 |
| 551.28 | 358.31 | 672.2 | 447.96 | 8.8356 |
| 510.09 | 330.68 | 627.5 | 415.92 | 9.5092 |
| 447.08 | 288.43 | 573.86 | 377.47 | 8.3408 |
| 402.6 | 258.59 | 529.16 | 345.43 | 8.4984 |
| 351.93 | 224.61 | 475.51 | 306.98 | 9.0767 |
| 302.97 | 191.78 | 430.81 | 274.94 | 8.6074 |
| 256.91 | 160.89 | 377.17 | 236.5 | 9.9213 |
| 208.15 | 128.18 | 332.46 | 204.45 | 9.4114 |
| 150.52 | 89.536 | 278.82 | 166 | 8.9747 |
| 103.51 | 58.004 | 234.11 | 133.96 | 8.7701 |
| 46.33 | 19.658 | 180.47 | 95.513 | 8.4305 |
| 20 | 2 | 144.71 | 69.882 | 9.9305 |
| 20 | 2 | 100 | 37.839 | 2.6051 |
| 20 | 2 | 50 | 2 | 2.2245 |

Table 3: Movement of sensor Node2 and Node1 and Their RSS values

| Node 1 | | Node 2 | | RSS Value |
|---|---|---|---|---|
| x | y | x | y | |
| 1155 | 794 | 1022 | 674 | 6.2389 |
| 1137.1 | 781.19 | 1022 | 674 | 8.0915 |
| 1110.3 | 761.96 | 1006.7 | 663.75 | 9.8261 |
| 1065.6 | 729.92 | 957.09 | 630.47 | 9.2409 |
| 1012 | 691.47 | 908.78 | 598.07 | 1.0336 |
| 958.31 | 653.02 | 841.33 | 552.83 | 8.44 |
| 922.55 | 627.39 | 807.42 | 530.09 | 8.811 |
| 868.9 | 588.94 | 759.4 | 497.89 | 9.8709 |
| 824.2 | 556.9 | 707.8 | 463.28 | 8.9724 |
| 770.55 | 518.45 | 648.99 | 423.84 | 8.4373 |
| 725.85 | 486.41 | 602.88 | 392.91 | 8.3896 |
| 672.2 | 447.96 | 551.28 | 358.31 | 8.8356 |
| 627.5 | 415.92 | 510.09 | 330.68 | 9.5092 |
| 573.86 | 377.47 | 447.08 | 288.43 | 8.3408 |
| 529.16 | 345.43 | 402.6 | 258.59 | 8.4984 |
| 475.51 | 306.98 | 351.93 | 224.61 | 9.0767 |
| 430.81 | 274.94 | 302.97 | 191.78 | 8.6074 |
| 377.17 | 236.5 | 256.91 | 160.89 | 9.9213 |
| 332.46 | 204.45 | 208.15 | 128.18 | 9.4114 |
| 278.82 | 166 | 150.52 | 89.536 | 8.9747 |
| 234.11 | 133.96 | 103.51 | 58.004 | 8.7701 |
| 180.47 | 95.513 | 46.33 | 19.658 | 8.4305 |
| 144.71 | 69.882 | 20 | 2 | 9.9305 |
| 100 | 37.839 | 20 | 2 | 2.6051 |
| 50 | 2 | 20 | 2 | 2.2245 |

Table 4: Movement of sensor Node1 and Node2 and Their RSS values

This completes our simulation results which show that RSS values are different according positions between nodes. Here Node1 is a common communicator between Node2 and Node3 still different RSS values gives us a random number generator (RNG).

A. Simulation in wireless Channel

In above section we have seen that initially nodes are static. At t= 2 ms, Node3 starts his mobility and moves towards location as X= 60, Y= 4, Z= 0. At t= 10 ms and t= 20 ms , Node2 and Node1 starts their mobility and moves towards location as X= 50, Y= 2, Z= 0, X= 20, Y= 2, Z=0 location respectively. All this simulation is simulated with the help of Shadow Propagation model which best as compared to Free-Space model or Two-ray ground propagation model.

Here sensor nodes get the same strength between each other and it’s different from other communicating nodes. All the nodes start their mobility after given time which immediately starts giving the different results for RSS values. Here no constraint is being kept on nodes movements.

Now we turn our discussion to graphical result simulation which will give the better idea of RSS calculated for different positions. We can see that values of both sides are sane i.e. from Node1 to Node3 and vice-a-versa. Same kind of observations can be noted for communication in-between Node1 and Node2. At the end we can conclude that RSS values from different communication links are different and it changes according to positions of communicating nodes.

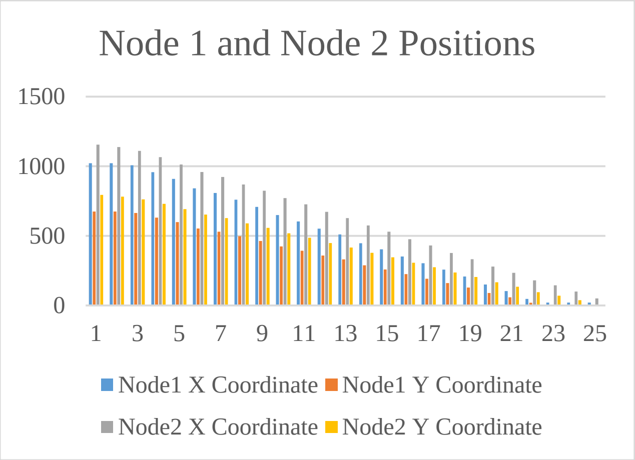

Fig. 1. Node 1 and Node 2 position variation

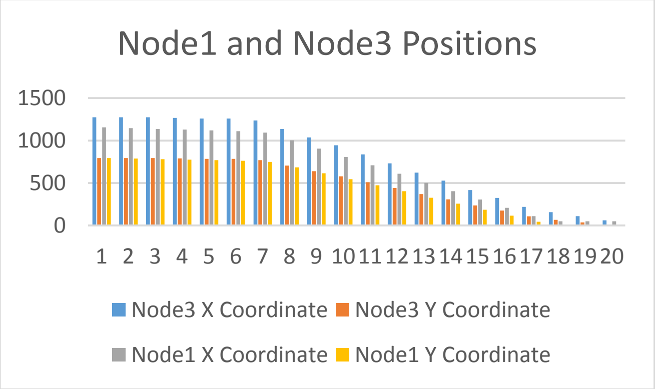

Fig. 2. Node 1 and Node 3 position variation

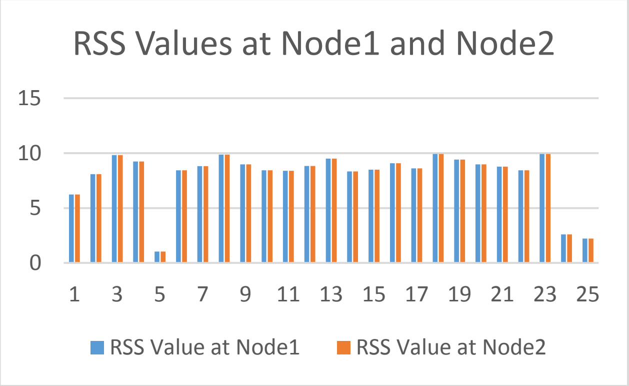

Fig. 3. RSS values at Node1 and Node2

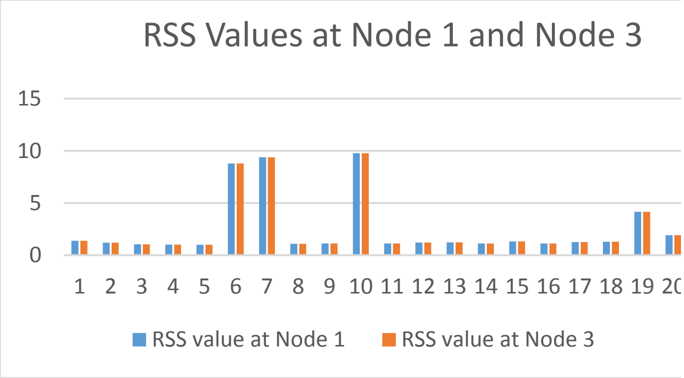

Fig. 3. RSS values at Node1 and Node2

## VI. CONCLUSION

At the end of all this discussion we can conclude that its possible to use RSS as random number generator which will eventually helpful to create the random cryptographic kr=ey for secure communication. As an enhacement or future scope we can do few additions also in the given architecture. Those can be as follows,

1. Defining proximity range of particular nodes and not the other nodes enter that particular region so that secrecy and impersonating is abandoned automatically.

2. If the network is about to fail because of any node has become dead then re-positioning the sensor nodes and calculating proximity ranges again where other nodes are not supposed to enter.

## REFERENCES

1. ZigBee Alliance. ZigBee specification. In Technical Report Document 053474r06. Version 1.0, June 2005.
2. J. E. Harshey, A. A. Hassan, W. E. Stark and S. Chennakeshu Cryptographic key argument for mobile radio. Elseveor Digital Signal processing, 1996.
3. A. Reznic C. Ye and Y. Shah Extracting secrecy from jointly Gaussian Random variables. July 2006.
4. A.Mercado B. Aazimi-Sadjadi, A. Kiayias and B.Yener. Robust key generation from signal envelopes in the wireless network. November 2007.
5. A.A. Hassan,J.E. Harshey and R.Yarlagadda unconventional cryptographic keying variable measurement.
6. A. Sayeed and A. Perigg: secure wireless communication: secret key through multipath. April 2008.
7. A. A. Hassan J. E. Hershey and R.Yarlagadd Unconventional cryptographic keying variable management.
8. S. W. Neville M. G. Madiseh, M. L. McGuire and A. A. B. Shirazi.: Secret key extraction in ultra wideband channels for unsynchronized radios. May 2008.
9. D. Tse R. Wilson and R. A. Scholtz. Channel identification: Secret sharing using reciprocity in UWB channels. September 2007.
10. Neal Patwari, Jessica Croft, Suman Jana, and Sneha K. Kasera. High rate uncorrelated bit extraction for shared secret key generation from channel measurements. IEEE Transactions on Mobile Computing, 2009.
11. N. Mandayam C. Ye S. Mathur, W. Trappe and A. Reznik. Radiotelepathy: Extracting a secret key from an unauthenticated wireless channel. September 2008.
12. T. Ohira B. Komiyama T. Aono, K. Higuchi and H. Sasaoka. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels. November 2005.
13. R. Miller Z. Li, W. Xu, and W. Trappe. Securing wireless systems via lower layer enforcement. September 2006.
14. CA. Network Simulator NS2 USC Information Sciences Institute, Marina del Rey. http://www.isi.edu/nsnam/nam. Last access, June 2009.
15. S. Jana and S. K. Kasera. On fast and accurate detection of unauthorized access points using clock skews. September 2008.
16. S. W. Neville M. G. Madiseh, M. L. McGuire and A. A. B. Shirazi. Secret key extraction in ultra wideband channels for unsynchronized radios. May 2008.