# Enhancement of Physical Layer Security by Exploiting Channel Phase Randomness in Wireless Networks

Varshinee Krishnamurthy, Ranjiny Natarajan Kumar, and Sivasankar Sundaram

***Abstract*—A less expensive and more flexible solution to the problem of sharing secret keys between wireless nodes is to use the inherent randomness in the wireless channel between them as the source for extracting bits of the secret key between these nodes. We propose a new secret key distribution approach that utilizes the uniformly distributed phase information of channel responses to extract shared cryptographic keys under narrowband multipath fading models. Compared to existing approaches which only support pair wise key distribution, our scheme is highly scalable and can support efficient group key distribution. Various key distribution schemes are appraised to determine the level of security and connectivity. Simulated results show that key distribution exploiting channel phase has improved resilience against node capture.**

***Index Terms*—Secret keys, resilience, randomness, multipath fading**

## I. Introduction

Wireless technology, by its nature, violates fundamental security principles. It does not ensure the identity of the user and the device (*authentication*), nor prevent the sender of the message from denying he or she has sent it (*non repudiation*).Many security breaches still occur because some newly introduced security protocols exhibit the vulnerabilities arising from the already known security problems. Traffic analysis is probably the easiest way to carry out a security attack. The attacker only listens to the data exchanged between two communication partners and does not bother whether he can understand it or not. However, under certain circumstances, the fact that two partners start to communicate or intensify their communication may already be valuable information. In addition, this attack may help you physically locate somebody or something in the network. The wireless networks are prone to many attacks like eavesdropping, masquerading, man-in-the-middle attack, Denial-of-service (DoS), Distributed DoS attacks.

Secret key establishment is a fundamental requirement for private communication between two entities. Currently, the most common method for establishing a secret key is by using public key cryptography. However, public key cryptography consumes significant amount of computing resources and power which might not be available in certain scenarios. A less expensive and more flexible solution to the problem of sharing secret keys between wireless nodes is to use the inherent randomness in the wireless channel between them as the source for extracting bits of the secret key between these nodes.

Shared secret key distribution from channel measurements is an application which benefits from the randomnessof the multipath channel. It would not, for example, work in a truly free-space environment (such as deep space radio links). Secret sharing benefits from:

• *Reciprocity of the wireless radio channel:* The multipath properties of the radio channel (gains, phase shifts, and delays) at any point in time and on any given frequency channel are identical on both directions of the link.

• *Temporal variations in the radio channel*: Over time, the multipath channel changes due to movement of either end of the link, and any motion of people and objects in the environment near the link. An application may specifically request a user to move or shake the wireless device in order to generate more temporal variation.

• *Spatial variations:* The properties of the radio channel are unique to the locations of the two endpoints of the link. An eavesdropper at a third location more than a few wavelengths from either endpoint will measure a different, uncorrelated radio channel. The proposed scheme is more flexible and can be applied in both static and mobile environments. Our scheme introduces phase randomness to bit distribution and removes the reliance on node mobility to obtain high entropy bits.

We evaluate the proposed schemes through both analytical and simulation studies. The parameters of the scheme can be selected such that a desired level of key distribution accuracy and reliability is achieved with high efficiency.

## II. Basic Schemes and Mathematical Models

Key distribution is an important issue in wireless network design. It is a newly developing field due to the recent improvements in wireless communications.

Random Key Predistribution: A network need not be fully connected for effective communication to take place. Hence it becomes unnecessary to store N-1 keys in every node as in pair wise key predistribution. Therefore random key predistribution is used, which ensures good connectivity in the network at the same time requires lesser memory space. Random key pre distribution schemes involve generating a large pool of symmetric keys from which a subset of keys is distributed to each node. The EG and DDHV schemes follow random key predistribution. [2].

Basically a key predistribution scheme has three phases, key distribution, shared key discovery and path-key establishment. During these phases, secret keys are generated, placed in nodes and each node searches the area in its

Manuscript received March 17, 2012; revised June 10, 2012.

The authors are with the Department of Electronics and communication Engineering, Anand Institute of Higher Technology, Chennai, India (e-mail: siva2eng@gmail.com)

DOI: 10.7763/IJFCC.2012.V1.101

communication range to find another node to communicate. A secure link is established when two nodes discover one or more common keys (this differs in each scheme), and communication between those two nodes takes place. Afterwards, paths are established connecting these links, to create a connected graph. The result is a wireless communication network functioning in its own way, according to the key predistribution scheme used.There are number of aspects of wireless networks on which key predistribution schemes are competing to achieve a better result. The most critical ones are: local and global connectivity, and resilience.

EG Scheme: Eschenauer and Gligor first proposed a random key predistribution scheme, which is also referred as basic scheme. Let m denote the number of distinct cryptographic keys that can be stored on a node. The basic scheme works as follows. In the initialisation phase a keypool is picked from the key space. Then a set of m key rings are assigned to each node. In the next phase , after the nodes are deployed , the nodes look for shared keys among them and then a link is established upon the discovery of common keys.

Eschenauer and Gligor calculate the necessary expected node degree din terms of the size of the network n as:

$$d = \left(\frac{n-1}{n}\right)(\ln(n) - \ln(-\ln(c))) \tag{2.1}$$

For a given density of network deployment, let nbe the expected number of neighbors within communication range of a node. Since the expected node degree must be atleast as calculated, the required probability pof successfullyperforming key-setup with some neighbour is:

$$p = \frac{d}{n'} \tag{2.2}$$

**DDHV Scheme:** The DDHVscheme [3], is based on a multiple key space scheme generated, which is randomly assigned to each node in the network. This is similar to Eschenauer and Gligor's assignment of randomly generated keys from a large key pool. In this scheme two nodes are able to calculate a unique pairwise key if and only if both nodes share a common key space. During the pre-deployment phase, a generator matrix G of size $(\lambda+1)\times N$ is created over a finite field GF(q) where q is an element within the finite field, N is the number of nodes in the network and $\lambda$ is a security parameter and , $s^k$ is a primitive or seed element of GF(q).

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 \\ s & s^2 & s^3 & s^N \\ s^2 & (s^2)^2 & (s^3)^2 & (s^N)^2 \\ s^\lambda & (s^2)^\lambda & (s^3)^\lambda & (s^N)^\lambda \end{bmatrix} \tag{2.3}$$

After the deployment phase, each node will attempt to identify its common-space neighbours by broadcasting a message that contains its unique node identifier. When using DDHV scheme in large networks, an adversary only requires to capture a relatively small number of nodes to compromise the network. This scheme is classified into two types: Grid based model and hexagonal based model.

### *A. Improving Key Predisrtribution Using Grid Based Deployment*

$$fi(x,y) = \frac{1}{2\pi\sigma^2} e^{\frac{-[(x-\mu xi)^2 + (y-\mu yi)^2}{2\sigma^2}} \tag{2.4}$$

where $\sigma^2$ is the variance of the distribution. However other distributions also can be used to model the deployment knowledge other than normal and uniform distribution.

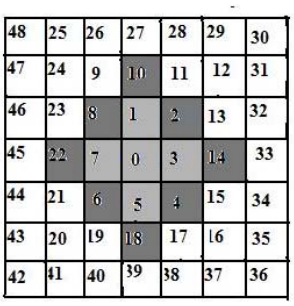


Fig. 2.1. Grid based model

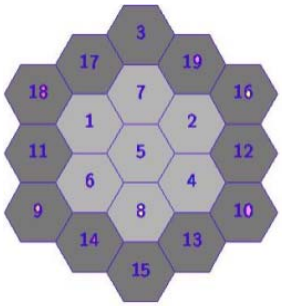


Fig. 2.2. Hexagon co-ordinate systems

Based on the deployment model shown in Fig 2.1, a group of nodes are deployed in a small local area, which causes most neighbours of a node come from its own group or neighbouring groups. The goal of this scheme is to allow nodes to find a common key with each of their neighbours after deployment.[4]

Key Predistribution Phase: The key predistribution phase is carried out before deploying the nodes in the area of interest. The field is divided into t groups. First the key pool S is divided into $t \times n$ key space pool, where n is the number of nodes. We say that two key-space pools are neighbours if their corresponding deployment groups are deployed in neighbouring (or nearby) locations. Once the key pools are generated, each node in the deployment group randomly picks up m keys from its corresponding key pool and load in its memory.

Shared Key Discovery Phase: After deployment, each node needs to discover whether it shares any key space with its neighbours by broadcasting the indices of the key spaces it carries. Each neighbouring node can use these broadcast messages to find out if there exists a common key space it shares with the broadcasting node. If such a key space exists, the two neighbouring nodes can derive a pair wise key from the common key space and use the key to secure the communication channel between them.Each node can communicate with the nodes deployed in 13 adjacent squares in the grid-based scheme as shown in Fig.2.1

Path Key Establishment Phase: If the nodes failed to find a common key, the nodes can establish pairwise keys in the path key establishment phase. When the node broadcasts the message ID the intermediate node can establish pairwise keys with the source and destination nodes. Otherwise, the intermediate node will broadcast the message till it share pairwise key with the neighbouring nodes. Then the path key is established.

### *B. Improving Key Predisrtribution Using Hexagon Based Deployment Model*

The centre of a grid is a deployment point, which is the

desired location of a group of nodes. The location of node over the entire field follows some distribution with a probability density function. In hexagon-based scheme, all adjacent nodes have the same distance. The hexagon system has some advantages over the rectangular system. First, when a node transmits data over wireless links, its signal range would form a circle that is centred around its deployment location with the radius being the distance of signal propagation. Therefore, a hexagon can be used to express and simulate the signal range more appropriately than a square can. Second, a hexagon can be used to describe equal distance between two neighbouring nodes. In a common rectangular coordinate system, the distance between neighbouring nodes differs, which depends on whether the neighbouring node is located directly adjacent (in which case the distance is 1 unit) or diagonal (in which the distance is square root of 2 units) to it. Under the hexagonal coordinate system, all adjacent nodes have that same distance which is normally 1 unit. According to the numbering rule, the numbers in the nth circle of the hexagon should be from $\sum_{i=1}^{n-1} 6(i-1)+1$ to $\sum_{i=1}^{n} 6(i-1)$. Consequently, we can determine a hexagon's location and its adjacent hexagons in a hexagonal coordinate system based on the above numbering rule.

Proposed Scheme: In dynamic scenarios where the two devices are mobile, and/or where there is a significant movement in the environment leads to random fluctuation in the phase and amplitude of the received signal. These random fluctuations attributes to the fading of wireless channels. Therefore, the temporal and spatial variations can be exploited to meet the security goals while the reciprocity property can be exploited for key distribution. Received signal strength (RSS) is a popular statistic of the radio channel and can be used as the source of secret information shared between a transmitter and receiver. The variation over time of the RSS, which is caused by motion and multipath fading, can be quantized and used for distributing secret keys.

The phase reciprocity of wireless communication can also be utilized for distributing keys. The security of the scheme is guaranteed based on the fact that it is infeasible for an adversary who is located at a different place with the transceivers to obtain the identical phase information for key distribution.Usually the signal being transmitted is degraded by the properties of the wireless medium. Therefore, in order to receive a safe and sound signal, the phase of the node should be well above the threshold. This notion is used to distribute keys and establish a secure link if a pairwise key exists.

Initially the node phases are determined for the defined set of nodes. The threshold is calculated and the keyspace is defined. From this , the keyrings are assigned to each node according to the nodephase value. Then common keys between nodes are found out and ultimately the links are established.

## III. Simulated Results

### A. Connectivity Analysis

*DDHV scheme:*

- Probability that two nodes share at least one key space is given by,

$$P(\lambda) = 1 - \frac{\sum_{k=0}^{min\ (\tau,\lambda|Sc|)} \binom{\lambda|Sc|}{k}\binom{(1-\lambda)|Sc|}{\tau-k}\binom{|Sc|-k}{\tau}}{\binom{|Sc|}{\tau}^2} \qquad (3.1)$$

The plot in Fig. 3.1 shows that when the probability of sharing at least one key space reaches 0.9996, no nodes were wasted and the local connectivity was improved as the memory usage increases.

Fig. 3.3 shows the local connectivity versus the number of keys (memory usage) each node carries. The analysis shows that the local connectivity of nodephase scheme can never reach one, because some neighbouring nodes might come from non-neighbouring deployment groups. With increasing memory usage, the probability of sharing at least one key space remains constant.

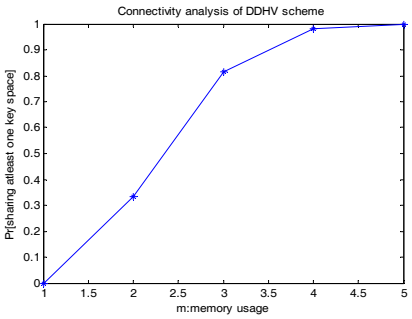


Fig. 3.1. Connectivity analysis of DDHV scheme.

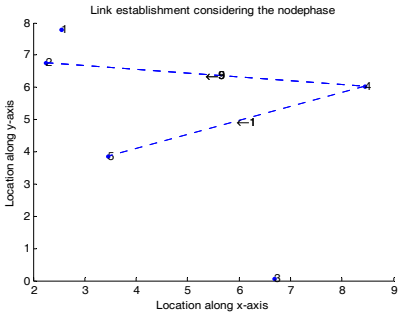


Fig. 3.2. Link establishment considering the nodephase

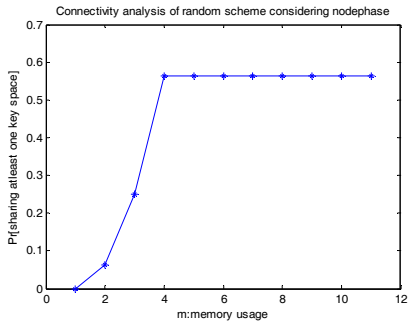


Fig. 3.3. Connectivity analysis of random scheme with nodephase

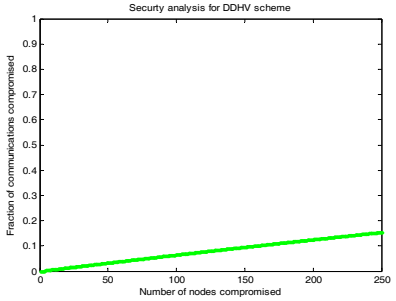


Fig. 3.4. Security analysis of DDHV scheme

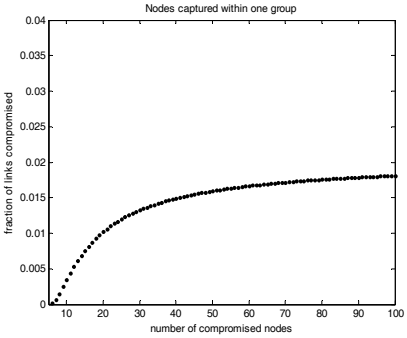


Fig. 3.5. Security analysis of random scheme with nodephase

### B. *Security Analysis*

The fraction of total keys being compromised can be expressed as,

$$P = 1 - \left(1 - \frac{m}{|s|}\right)^{x} \qquad (3.2)$$

The Equation (3.2) implies smaller the value of m, better the resilience. Such an improvement is attributed to the deployment knowledge, which enables usto reduce the number of unnecessary keys carried by each node. Fig.3.4 illustrates the security analysis of DDHV scheme.

Fig. 3.5 shows the security analysis of nodephase based scheme within one group. Almost 2% of links iscompromised in the channel phase based scheme

From the results we infer that, though the connectivity of the basic scheme is higher than the proposed scheme, it is vulnerable to security threats leading to poor resilience. where as in the proposed scheme , the security is enhanced by compromising connectivity.

## IV. CONCLUSION:

In this paper, we propose a new secret key generation approach that utilizes the uniformly distributed phase information of channel responses to distribute shared cryptographic keys under narrowband multipath fading models. The proposed approach achieves scalability and flexibility.

## REFERENCES

[1] Q. Wang et al, “Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks,” in P*roc. IEEE INFOCOM ’11*, 2011

[2] S. Jana et al, “On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments,” in *Proc. Mobi Com ’09*, Sept. pp. 321–32, 2009.

[3] B. A. Sadjadi et al, “Robust Key Generation from Signal Envelopes in Wireless Networks,” in *Proc. CCS ’07*, pp. 401–10, 2007.

[4] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, “A Key Predistribution Scheme for Sensor Networks using Deployment Knowledge,” *IEEE transactions on Dependable and Secure Computing*, vol. 3, no. 1, pp.62-77, 2006 .

[5] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge,” in *IEEE INFOCOM*., 2004.