Time-Dependent Key Generation Method Based on Secure Wireless Communication

Remya M Nair

Assistant Professor, Dept. of ECE, SHM Engineering college Kollam, India

remyamn27@gmail.com

Abstract— Security is an important issue in wireless communication systems as the wireless channel is unguided. Cryptographic techniques in the wired communication may be used to secure the wireless communication, but the characteristics of radio channel are not exploited efficiently. This project presents a synchronized random key generation for each node which depends on the clock time. So there is no need any key transfer. Key generation protocol is used here. Key generation protocol depends on the global timing method. Here we use base station time as a global time. Pseudo random number creation depends upon the time and the initial value of linear feedback shift register. So each and every second create a new key. So the level security is too high and power consumption is very low.

Keywords— cryptography, wireless communication, Encrypt, decrypt, network security, shift register, GPS, MATLAB

INTRODUCTION

The development of wireless communications and wireless networks is very rapid in recent years, varieties of wireless applications continue to emerge. However, it is more difficult to secure wireless communications than wired communications as the wireless channel is unlimited. Securing the wireless communication is an extremely important aspect almost in every wireless communications system.

The classical cryptography is used to secure the wired communication. Two types of cryptographic techniques are used: public key cryptography and secret key cryptography. The transmitter converts the plaintext to encrypted message using public or private keys in the application layer. However, distributed parallel computing makes the public key cryptography become unsafe. Hence, the security of private keys determines the security of the systems for the secret key cryptography.

The basic idea is that the node receives a random vector and a master key before deployment. Any two nodes are able to establish their pair wise key by combining their vectors with the master key. In this way, the proposed scheme solves three problems: the node establishes its pair wise keys independently, rather than search for it passively; as a result, any two nodes could establish a pair wise key, and the problem on connectivity is solved. By using a random vectors and a master key to establish the pair wise keys, the node needn’t store a lot of keys. Therefore, the memory overhead has been reduced. As the probability that any two nodes receive the same vector in network is quite low, it can be make sure that all the pair wise keys are different with each other, so the network’s resilience to the capture attack has been enhanced.

LITERATURE SURVEY

Wireless Communication

Wireless communication is, by any measure, the fastest growing segment of the communication industry. As such, it has captured the attention of the media and the imagination of the public. Cellular phones have experienced exponential growth over the last decade, and this growth continues unabated worldwide, with more than a billion worldwide cell phone users projected in the near future. Indeed, cellular phones have become a critical business tool and part of everyday life in most developed countries, and are rapidly supplanting antiquated wire line systems in many developing countries.

In addition, wireless local area networks are currently poised to suppliment or replace wired networks in many businesses and campuses. Many new applications, including wireless sensor networks, automated highways and factories, smart homes and appliances, and remote telemedicine, are emerging from research ideas to concrete systems. The explosive growth of wireless systems coupled with the proliferation of laptop and palmtop computers indicate a bright future for wireless networks, both as stand-alone systems and as part of the larger networking infrastructure. However, many technical challenges remain in designing robust wireless networks that deliver the performance necessary to support emerging applications.

Network Security

In the field of networking, the special area of network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources .The terms network security and information security are often used interchangeably. Network security is generally taken as providing protection at the boundaries of an organization by keeping out intruders (hackers). Information security, however, explicitly focuses on protecting data resources from malware attack or simple mistakes by people within an organization by use of data loss prevention (DLP) techniques. One of these techniques is to compartmentalize large networks with internal boundaries.

The terms network security and information security are often used interchangeably. Network security is generally taken as providing protection at the boundaries of an organization by keeping out intruders (hackers). Information security, however, explicitly focuses on protecting data resources from malware attack or simple mistakes by people within an organization by use of data loss prevention (DLP) techniques. One of these techniques is to compartmentalize large networks with internal boundaries.

Network security starts from authenticating the user, commonly with a username and a password. Since this requires just one thing besides the user name, i.e. the password which is something you 'know', this is sometimes termed one factor authentication. With two factor authentication something you 'have' is also used (e.g. a security token or 'dongle', an ATM card, or your mobile phone), or with three factor authentication something you 'are' is also used (e.g. a fingerprint or retinal scan).

Cryptography

Cryptography is the practice and study of techniques for secure communication in the presence of third parties . More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Cryptology prior to the modern age was almost synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The sender retained the ability to decrypt the information and therefore avoid unwanted persons being able to read it. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasing complex and its application more widespread.

Secret key Cryptography:

With secret key cryptography, a single key is used for both encryption and decryption. As shown in Figure 1A, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or rule set) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret. The biggest difficulty with this approach, of course, is the distribution of the key .Secret key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing. A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same cipher text when using the same key in a block cipher whereas the same plaintext will encrypt to different cipher text in a stream cipher.

Random Key Generation

Key generation is the process of generating keys for cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/ decrypted. Modern cryptographic systems include symmetric-key algorithms (such as DES and AES) and public-key algorithms (such as RSA). Symmetric-key algorithms use a single shared key; keeping data secret requires keeping this key secret. Public-key algorithms use a public key and a private key. The public key is made available to anyone (often by means of a digital certificate). A sender encrypts data with the public key; only the holder of the private key can decrypt this data.

Since public-key algorithm tend to be much slower than symmetric-key algorithms, modern systems such as TLS and SSH use a combination of the two: one party receives the other's public key, and encrypts a small piece of data (either a symmetric key or some data used to generate it). The remainder of the conversation uses a (typically faster) symmetric-key algorithm for encryption.

SYSTEM DESIGN

Establishment of Keys

The establishment of keys consists of four phases; including initialization, pair wise key establishment, cluster key establishment and station key establishment. The meanings of each phase are as follows:

Initialization

Before deployment, the node receives a master key K, a node identifier Id and a random vector ‘a’. Firstly, generate a k-dimensional vector group A,

$$A=(\,\mathbf{a1} \quad \mathbf{a2} \quad \mathbf{\ldots\ an}\,)$$

where, **a1, a2, an** represents the vectors in a vector group which is represented as a string.

Each vector of A is generated by the random number generator, ai(0, 1). Every node receives a vector ai from vector group A at random without replacement. In addition, the node should also receive other information, including the master key and a random number generator.

Pairwise Key Establishment

The pair wise key is generated between two nodes which are obtained by the grouping of vectors from each node with the master key. The key is generated by combining the diagonally available strings. The matrix is a symmetric matrix and it is said to contain two bit strings as its elements.

Generally the matrix for key generation is given as

$$K=\left(\begin{tikzcd} aii \arrow[dr] & aij & aik \\ aji & ajj \arrow[dr] & ajk \\ aki & akj & akk \end{tikzcd}\right)$$

i.e., K is the concatenation of aii, ajj, akk

The first row denotes the Master key, the second row denotes the transmitting node’s vector and the third row denotes the receiving node’s vector.

Cluster Key Establishment

The cluster key is generated between the cluster-head and a node which is obtained by the grouping of the vectors from the node and cluster-head with that of the master key.The cluster-head is selected by means of the estimation of energy consumption by nodes.

Mathematical Expression

The general mathematical expression for the generation of the key can be given as

$$T(K)=aii+ajj+akk$$

Here T(K) represents the trace of a matrix. Trace of a matrix is nothing but combining the diagonal strings of a matrix.The key is generally formed by combining the first two bits of the Master key, the next two bits of the transmitter node and the last two bits of the receiving node.

Block Diagram

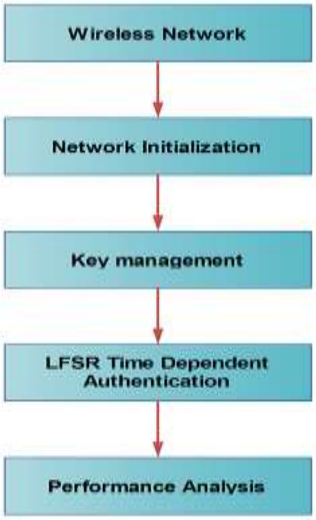


Fig. 1. Block Diagram of Time-Dependent Key Generation Method **.**

4.5 Authenticate Data Update

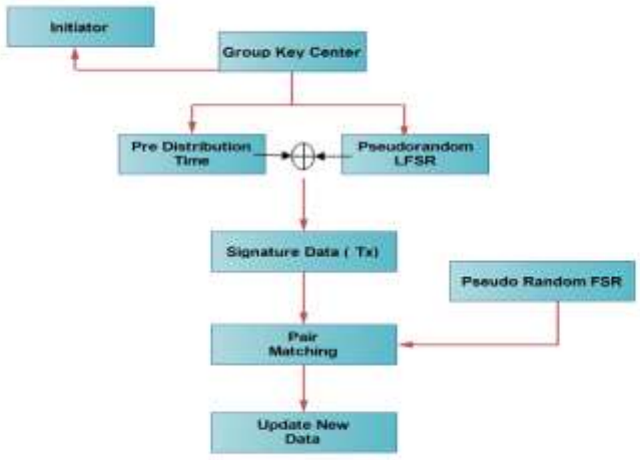


Fig. 2. Authenticate Data Update

In the case of the pair wise key establishment, both the transmitter and the receiver are nodes while in the case of the cluster key establishment, the transmitter is a node and the receiver is the cluster-head and in the case of the station key the cluster-head is the transmitter and the receiver is the Base station.Our proposed scheme is based on Level architectural routing which mainly reduces the memory overhead and provides security.

System Model

This paper compare the simple location dependend key generation method using multiple antenna and time dependend key generation for secure wireless communication.

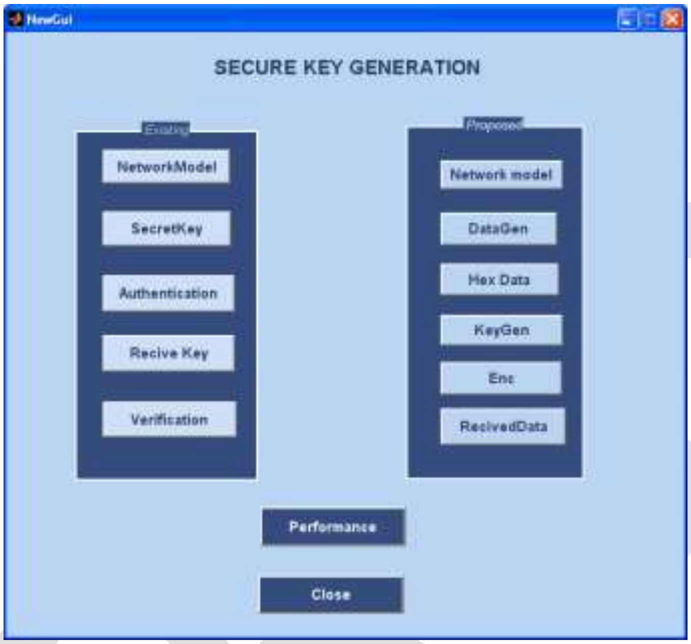


Fig. 3. System Model

In the existing system we are using multiple antennas for measuring the distance between the nodes. If the distances are same, they will start data transfer. In the existing work, there will be a key generating center that will send key updating request to the base station.

Result And Discussion

The base station will send that request to the nodes that are included in the communication.

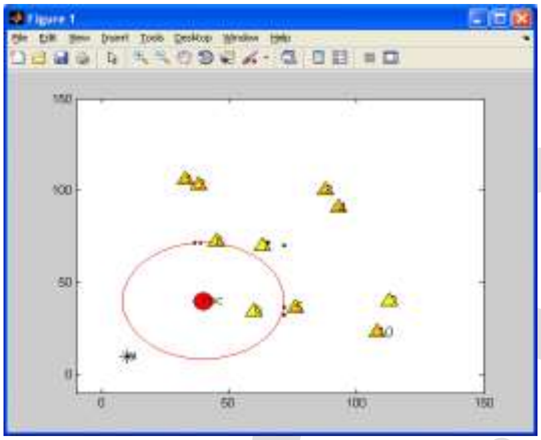


Fig.4. Key Generating Center asking for key updation

Then the nodes will send the acknowledgement to the base station. Then the secret data will be generated and send to the nodes

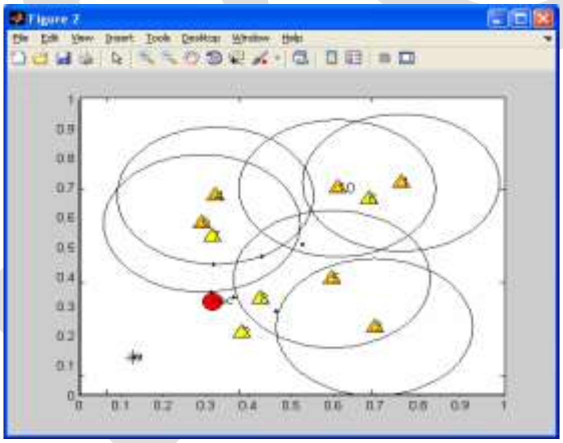
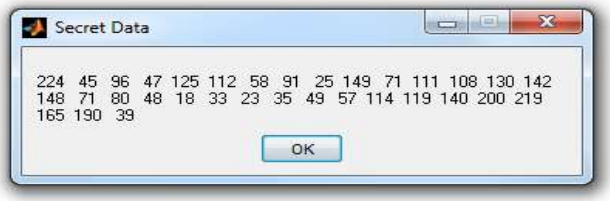


Fig.5. Acknowledgement send by the nodes

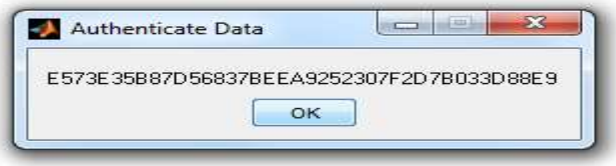
The secret data will send into the nodes. Secret data will be encrypted and then send to the nodes.



```
224  45  96  47 125 112  58  91  25 149  71 111 108 130 142
148  71  80  48  18  33  23  35  49  57 114 119 140 200 219
165 190  39
```

Fig.6.Secret Data

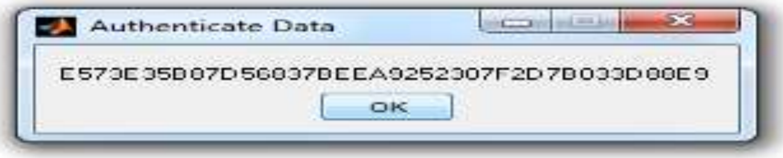
The authenticate data will received by the nodes.



E573E35B87D56837BEEA9252307F2D7B033D88E9

Fig.7. Authenticate Data at the transmitter side.

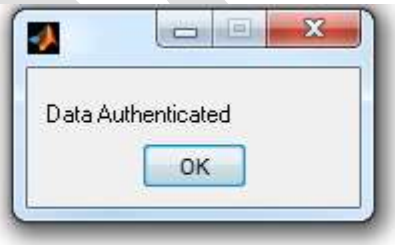
At the receiving side, the received data is decrypted and the data will be the same



E573E35B87D56837BEEA9252307F2D7B033D88E9

Fig.8. Authenticate Data at the receiver side

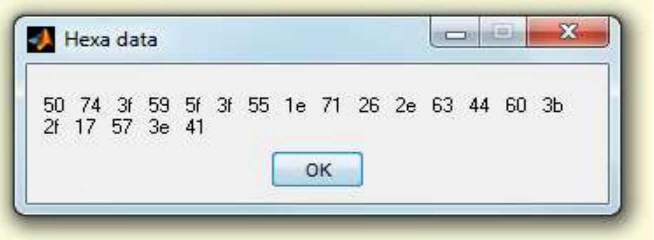
Thus the data is authenticated without any change.



Data Authenticated

Fig.9.Data Authentication

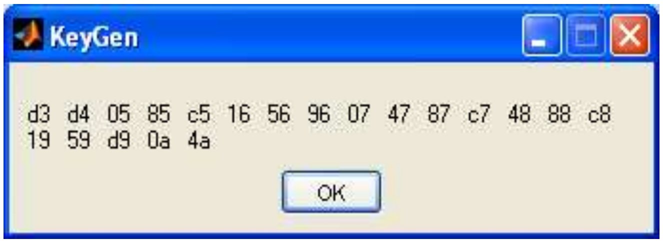
In the proposed work, there will be no key transfer. Some binary data will be generated and we will convert it into hexadecimal number.



```
50  74  3f  59  5f  3f  55  1e  71  26  2e  63  44  60  3b
2f  17  57  3e  41
```

Fig. 10. Hexadecimal equivalent for data generated

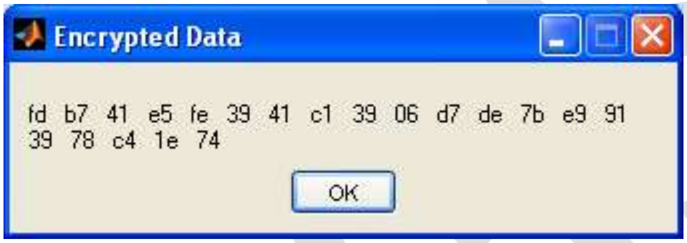
Then a key is generated using LFSR. Then we will convert the key into hexadecimal number.



```
d3  d4  05  85  c5  16  56  96  07  47  87  c7  48  88  c8
19  59  d9  0a  4a
```

Fig. 11. Key generated by the LFSR

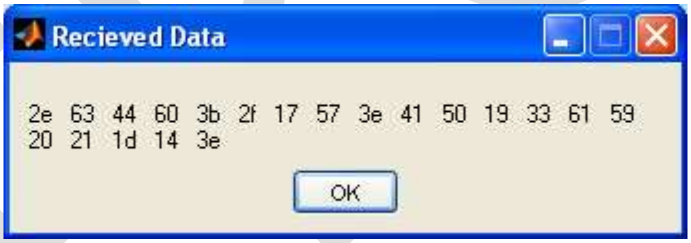
Secret data is encrypted using the key generated



```
fd  b7  41  e5  fe  39  41  c1  39  06  d7  de  7b  e9  91
39  78  c4  1e  74
```

Fig. 12. Encrypted data

At the receiving side the data will be decrypted and we will get the same data.



```
2e  63  44  60  3b  2f  17  57  3e  41  50  19  33  61  59
20  21  1d  14  3e
```

Fig.13. The data that is decrypted by the receiver

Performance Chart

Compare the performance of the proposed work with the existing work, delay in the network will be less in the proposed work as the nodes communicate directly.

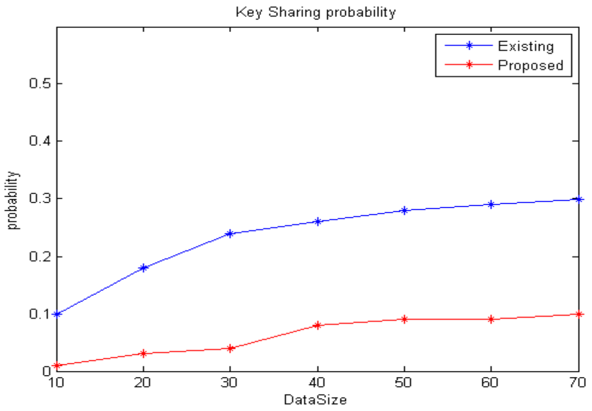


Fig.14. Key Sharing Probability

Compare the delay and data size of proposed and existing work. Delay in the proposed network will be less, because the nodes communicate with each other directly.

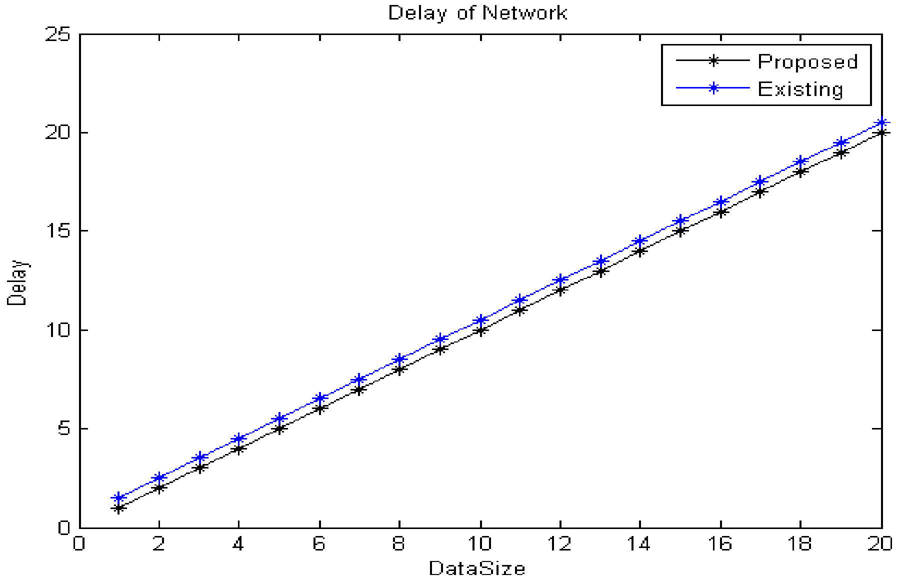


Fig.15. Delay of Network

CONCLUSION

In the key pre-distribution schemes a large quantity of keys are needed to establish the shared key, that causes great memory overhead; an attacker could capture a node and attack the network using the subset of keys. These problems have been rectified in the proposed key management scheme that is based on vector group, which is able to establish the pair wise keys independently. It provides a better security performance with a low memory overhead.

Simulation results show that the proposed scheme could establish all the keys by one- broadcast, and reduce the communication overhead , the energy consumption has been effectively reduced; the probability that any two pair of nodes establish the same pair wise key has been decreased to 0, accordingly, the threat of node capture has also been reduced, and the security of the network has been improved; the perfect memory overhead of nodes in WSN is only to store the pair wise keys related to its neighbors. In the proposed scheme, the memory overhead approximately equals to the node degree, therefore, it has a lower memory overhead than typical key pre-distribution schemes. Moreover in the proposed scheme, we only use binary arithmetic to generate keys and hence it is easy to calculate and cause less energy consumption.

REFERENCES:

[1]Jianguo Zhang, Qinye Yin, Pengcheng MU” A Simple Location-dependent Key GenerationMethod Based on Multiple Antennas for SecuringWireless Communication” in proc. ICACT2011 .p.992

[2] R. Wilson, D. Tse and R. A. Scholtz,, "Channel identification: secret sharing using reciprocity in ultrawideband channels," IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, pp. 364 -375, Sep. 2007.

[3] M Shin, J Ma, A Mishra, et al., "Wireless network security and interworking," Proceeding of the IEEE, vol. 94, no. 2, pp. 455-466, Feb. 2006.

[4] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, et al., "Robust key generation from signal envelopes in wireless networks," in Proc. ACM CCS '07, 2007, p 401.

[5] X. Li, J. Hwu, E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," Journal of Communications, vol. 2, no. 3, pp. 24-32, Mar. 2007

[6] . J. W. Wallace, C. Chen, and M. A. Jessen, "Key generation exploiting MIMO channel evolution: algorithms and theoretical limits," in Proc. EuCAP'09, 2009, p. 1499.

[7] N. Vereshchagin, "A new proof Ahlswede - Gacs - Korner theorem on common information," Tech. Rep., September 2002, ´ http://lpcs.math.msu.su/˜ver/papers/gka.ps.

[8] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," Digital Signal Processing, vol. 6, pp. 207–212, Oct. 1996.

[9] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," Trans. on Communications, vol. 43, pp. 3–6, Jan. 1995.

[10] M. A. Tope and J. C. McEachen, "Unconditionally secure communications over fading channels," in Proc. MILCOM. IEEE, 2001, pp. 54–58.

[11] A. F. Molisch, J. R. Foerster, and M. Pendergrass, "Channel models for ultrawideband personal area networks," Wireless Communications, pp. 14–21, Dec. 2003.

[12] J. G. Proakis, Digital Communications, 4th ed. New York, NY: McGraw-Hill, 2001.