International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Proposed Paper for D-Scrabble Physical Layer Security Model Integrated with AI

Devansh Dave

K.J.Somaiya College of Engineering, Mumbai, India

Abstract: ***This paper proposes a new model for enhancing physical layer security. In today's world, cryptography and encryption algorithms like RSA and Diffie-Hellman can be broken down by high computation capability of computers. Inclusion of security in physical layer will greatly reduce the problem of eavesdropping and wiretapping. The main idea is to prevent security attacks from its root itself. The strength of any encryption algorithm or security model lies in its nature of unpredictability and adaptability. This paper puts forth idea of integrating AI with physical layer security. Human's way of thinking is the most unpredictable pattern. Scrabble, a puzzle word game, is used to humanize the D-Scrabble model and thus introduce a strong security model with great level of unpredictability. A new method called cycling technique is also introduced in this paper. This model also uses a new technology, NEAT-NeuroEvolution of AugmentingTechnologies.***

Keywords: NEAT- NeuroEvolution of Augmenting Technologies, Scrabble, AI, Physical layer security, encryption, Security with AI

1. Introduction

1.1 Cryptography and Encryption algorithms:

Diffie-Hellman key exchange is a popular cryptographic algorithm that allows Internet protocols to agree on a shared key and negotiate a secure connection. Diffie-Hellman key exchange is widely used to establish session keys in Internet protocols. It is the main key exchange mechanism in SSH and IPsec and a popular option in TLS [3].

But there are some weaknesses in it as follows:

a) **Logjam attack against the TLS protocol.** The Logjam attack allows a man-in-the-middle attacker to to read and modify any data passed over the connection [3].
b) **Threats from state-level adversaries.** Millions of HTTPS, SSH, and VPN servers all use the same prime numbers for Diffie-Hellman key exchange [3]. Practitioners believed this was safe as long as new key exchange messages were generated for every connection. However, the first step in the number field sieve—the most efficient algorithm for breaking a Diffie-Hellman connection—is dependent only on this prime. After this first step, an attacker can quickly break individual connections [3].

Hence, Encryption algorithms are no longer fully secure so Physical layer security was introduced to increase the security measures.

1.2 Scrabble

Scrabble is a famous word-puzzle game which requires a mixture of vocabulary, strategy, pattern- recognition and luck. This game where luck and outside knowledge also play a role. There are high number of permutations and combinations made to find highest possible scoring word from the word dictionary. The other important point is speeding up AI. Various algorithms should be made considering the behavioral patterns. The player can play many times and store the statistics to improve the gameplay of AI.

Scrabble is an appropriate game for security model because the patterns and the time at which the word is solved helps in creating unique patterns and ordering of frames, thus introducing a great level of unpredictability.

2. Previous Work

2.1 Physical Layer Security

Physical-layer security utilizes resources of the transmission medium to guarantee secure communication against an adversary with unlimited computational power [6]. Computational security approaches have worked well in practice although there is continuing effort to test their limits in terms of the computation power needed to break them [6].

The fundamental principle behind physical layer security is to exploit the inherent randomness of noise and communication channels to limit the amount of information that can be extracted at the „bit" level by an unauthorized receiver [5]. This model also works at bit-level.

2.2 Trusted Third party (Certificate Authority)

Trusted third parties can be useful in a variety of tasks in distributed systems. For instance, certification authorities are helpful in associating public keys with the names of users and other principals; in multi-player games, servers can contribute to preventing some forms of cheating; and smart-cards with limited resources may rely on trusted, off-card servers for verifying downloaded bytecode class files [4].

The trusted third party can contribute to secrecy properties, for example holding secrets for a user, and presenting those secrets only to appropriate remote servers [4]. The secrets would be kept from viruses that may come with arbitrary programs. The trusted third party can also contribute to integrity properties, for example checking incoming and outgoing data [4].

2.3 NEAT- NeuroEvolution Augmenting of Topologies:

Traditionally when using genetic programming, a neural network topology is designed by a human experimenter, and a genetic algorithm is used to learn effective connection weight values for it, However, this approach does not modify the topology of the network [1].

NeuroEvolution of Augmenting Topologies (NEAT) is a genetic algorithm for the generation of evolving artificial neural networks. NeuroEvolution (NE), the artificial evolution of neural networks using genetic algorithms, has shown great promise in complex reinforcement learning tasks [2].

The NEAT approach begins with a perceptron-like feed-forward network of only input neurons and output neurons. As evolution progresses through discrete steps, the complexity of the network's topology may grow, either by inserting a new neuron into a connection path, or by creating a new connection between (formerly unconnected) neurons [1]. The first application of rtNEAT is a video game called Neuro-Evolving Robotic Operatives, or NERO. In the first phase of the game, individual players deploy robots in a 'sandbox' and train them to some desired tactical doctrine. Once a collection of robots has been trained, a second phase of play allows players to pit their robots in a battle against robots trained by some other player, to see how well their training regimens prepared their robots for battle [1].

player has to periodically play and update its database with new final boards so that new Scrabble patterns are generated and ensures freshness in the process. The selected unique Scrabble pattern can also be called as *adapt key* because it adapts as the player thinks.

The following steps are followed here-:

1) Alice intends to start communication with Bob. So TTP authenticates Alice and gives public key of Bob.
2) Then, TTP side player plays Scrabble with AI. It should not necessarily play when a request comes up. It can select a pattern from last finished board. The finished board is ready.
3) Alice sends its network specification information to TTP.
4) TTP prepares a data file consisting of information related to the unique Scrabble pattern or the encrypted image

3. Proposed Model For D- Scrabble

The D-Scrabble security model has been devised to cater to different security needs. There are primarily two basic models:
a) Public D-Scrabble: This model is targeted for people with lesser security measures and reasonable price. Public model will only have an AI on TTP side and not on either of the communicating sides. The only difference between the two models is the inclusion of NEAT AI on the communicating sides and TTP in Private model.

3.1 Public (without NEAT AI):

The main players in this model are:
1) Communicating sides Alice and Bob
2) Trusted Third Party
3) AI on TTP side.

Explanation:
This model requires a human to play Scrabble with AI and complete it. It has to store the final finished board in its database. Then upon any communication request it has to randomly recognize patterns suitable to network specifications sent by the communication initiator. Network specifications primarily mean the data size, frame size and capacity, synchronization time, encoding techniques and various other parameters. The selected unique Scrabble pattern based on initiator‟s network specifications is sent to initiator in the form of encrypted .zip data file. The
itself. It then zips the file and
5) After obtaining the unique Scrabble pattern, it initiates communication with Bob.
6) TTP authenticates Bob and gives public key of Alice.
7) Bob also sends its network specifications to TTP.
8) TTP upon identifying that the communicator is Bob gives exactly the same Scrabble pattern mapped to Alice in encrypted .zip data file.
9) After obtaining their Scrabble patterns, they continue communication by arranging and hiding data bits according to the Scrabble pattern in the data link layer. Hiding in the sense means hiding the bits by cycling technique explained in framing scenario section.

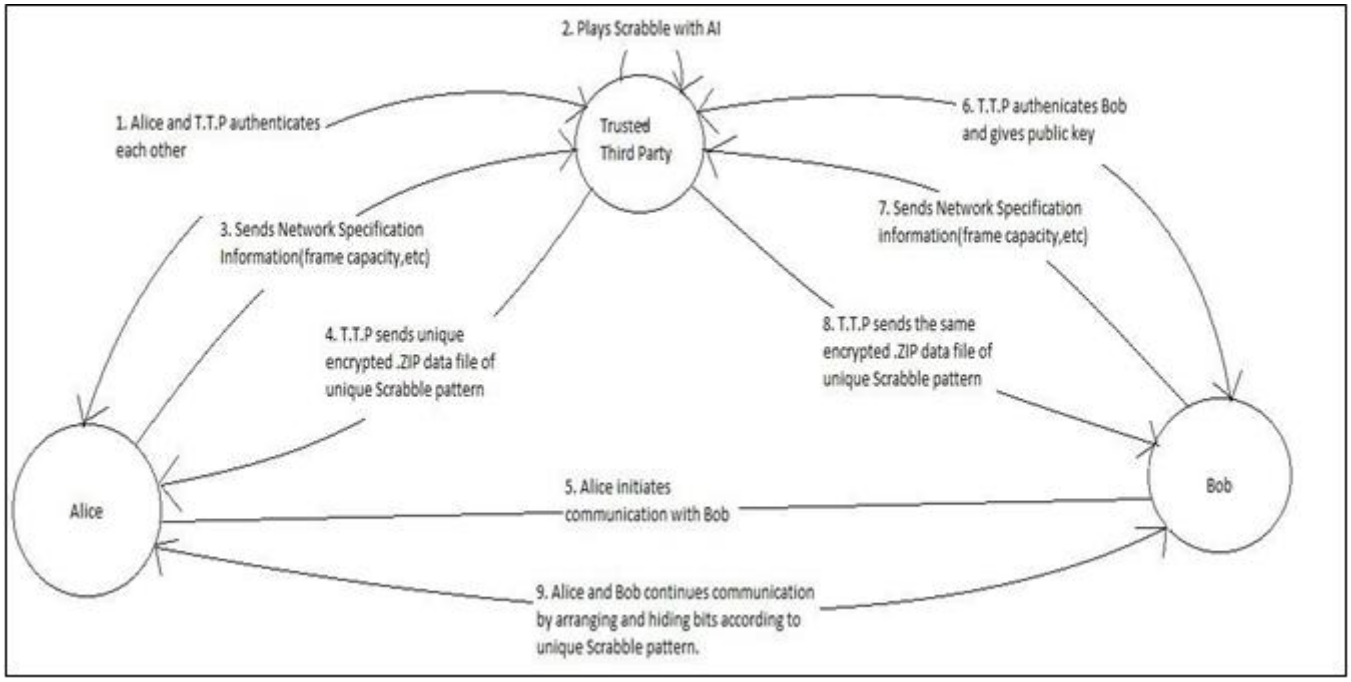


Figure 1: Public D-Scrabble model

3.2 Private (with NEAT AI):

The main players in this model are:

1) Communicating sides Alice and Bob encrypts it to send. It also stores the particular with a unique id and maps it to initiator Alice.
2) Trusted Third party
3) NEAT AI and Database at all the three sides

Explanation: This model is designed for highly secure communication like governmental talks or messages, company‟s confidential matters, money transactions, sharing of secret key, etc. This can be expensive but offers higher security as NEAT AI is needed on the communicating sides too. This arise the need to have database and high processor capability as complexifying logic is periodically sent to Alice and Bob. Alice and Bob require having initial database pertaining to TTP. Then TTP sends the same complexifying logic as *adapt key* to Alice and Bob so that when the AI on their side play Scrabble they produce same unique patterns. This is an ideal security model because the unique Scrabble pattern is never transmitted over channel but both parties predict the pattern themselves with the help of their AI. The inclusion of NEAT AI makes it self-evolving.

The steps followed in this model are same as public model except four main points:

1) TTP sends complexifying logic to Alice instead of unique Scrabble pattern as in public model.
2) The AI at Alice and Bob plays Scrabble and forms its own pattern to communicate with each other as opposed to public model where they obtain the pattern from TTP.
3) The database with Alice and Bob has to be updated with the new logic given by TTP.
4) NEAT AI is a self-evolving neural network so as an added precaution, Alice and Bob can exchange reconfirmation messages to be sure of the correct data.

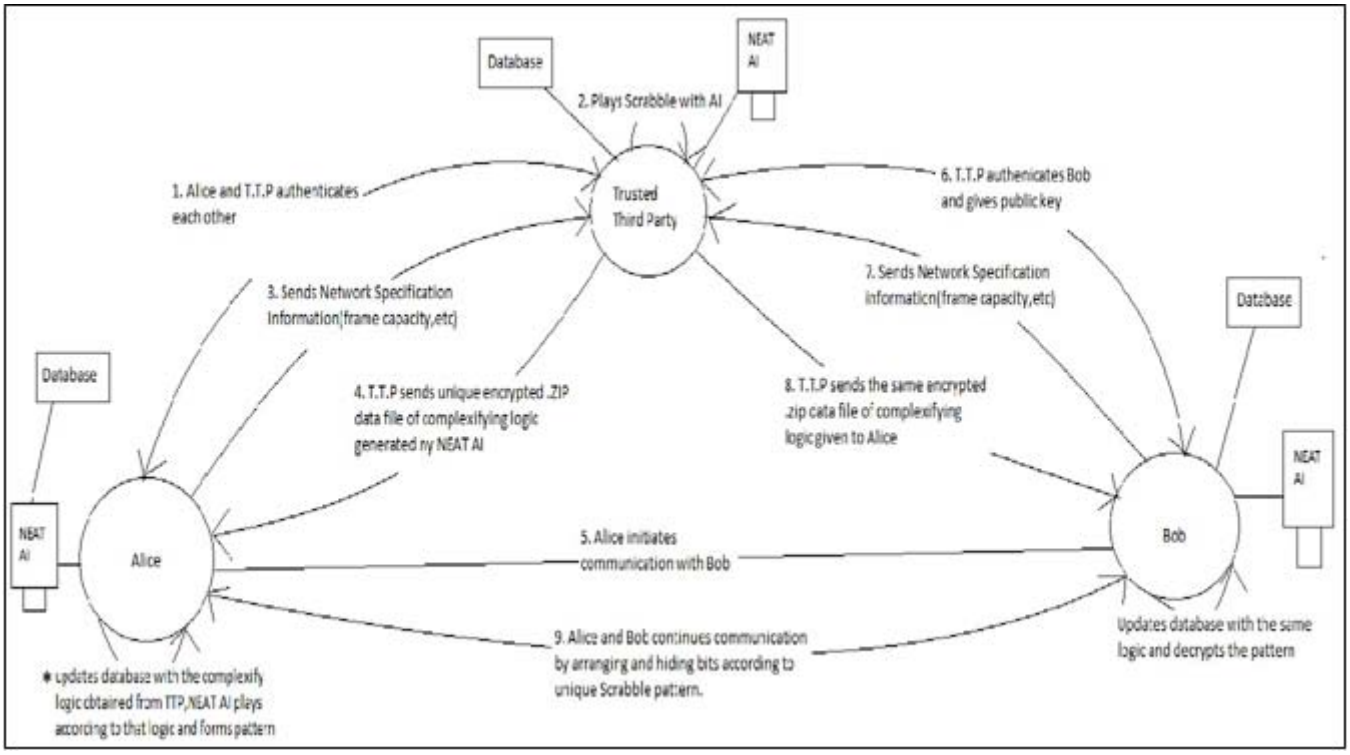


Figure 2: Private D-Scrabble model

3.3 Framing scenario

The Scrabble pattern obtained is applied on data bits to properly order and hide data bits. The data bits are altered according to the pattern and then packed in frames. There are primarily three basic steps to implement our model-:

1) First obtain the Scrabble pattern from TTP and encrypted .zip data file containing encrypted Scrabble pattern image and various other information related to it as in Figure 3. The time when the word was made to solve the puzzle is recorded and ordered accordingly. As in the figure ROSE was solved first so while transmitting it will be placed first.

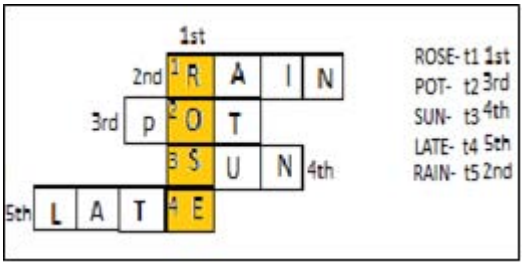


Figure 3: Scrabble pattern and word solving time

2) The actual meaningful frames are matched and placed in the Scrabble pattern as shown in Figure 4. The appropriate pattern matching algorithm should be used to properly devise Scrabble pattern matched frames.

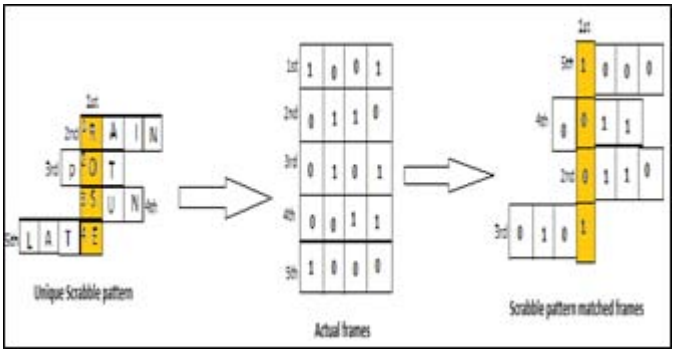
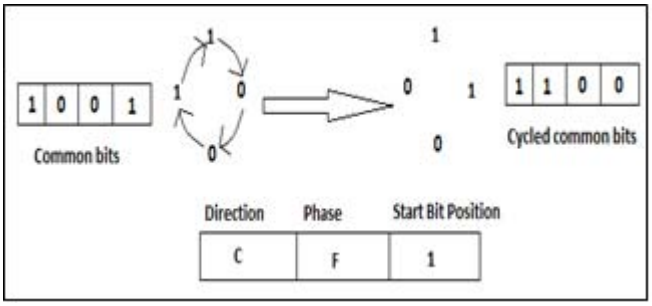


Figure 4: Scrabble pattern matching

3) The next step is to hide the common bits in Scrabble pattern matched frames. The common bits are the same as the overlapped word in Scrabble word- puzzle game (as in figure. ROSE). These bits are hidden from eavesdropper by a cycling technique as given in Figure 6. Cycling technique is a method in which these common bits are applied the following parameters:

i) Anticlockwise/Clockwise direction-: The chosen bits should be transmitted in one of the following direction.
ii) Start bit: The start bit should be specified appropriately as these can change the meaning.
iii) Full/Half/Quarter phase: This divides the bits into half or quarterly or none. This gives the technique more complexity. Quarterly phase means the bits are divided in four parts and four start bits are chosen along with direction.
Figure 6: cyclic technique



iv) Ultimately, with application of Scrabble pattern matching and cycling technique, the frames are ordered in accordance with the time their corresponding Scrabble words were solved. The time has been shown in figure 5.

While decrypting it at Bob‟s side, he has to just apply the phases from the start bit in opposite direction. This information related to the cyclic parameters is sent to Bob and Alice from the TTP.

4. Possible Attack Scenario

The D-Scrabble model has several layers of security. An attacker has to penetrate all this layers to target an attack on the individual. The five layers of model are-

1) Pattern layer: The pattern created is unique and unpredictable because it is something created by human‟s way of thinking.
2) Ordering layer: The frames are ordered according to the time at which the player solves puzzle with the particular word associated with that frame. This is also very unpredictable.
3) Cyclic technique layer: The common bits are stored separately and with the help of cyclic technique they are rotated from start with either of the phase. This technique is very helpful for large bit frames.
4) Encrypted .zip data file: This .zip encryption helps in increasing the security level and is appropriate for carrying this model‟s sensitive information. The invention in the paper [7] relates generally to a method of using standard .ZIP files and strong encryption technology to securely store files, and more particularly to a method of integrating existing strong encryption methods into the processing of .ZIP files to provide a highly secure data container which provides flexibility in the use of symmetric and asymmetric encryption technology [7].

The invention in the paper [7] adapts the well established and widely used .ZIP file format to support higher levels of security and multiple methods of data encryption and key management, thereby producing an efficient, highly secure and flexible digital container for electronically

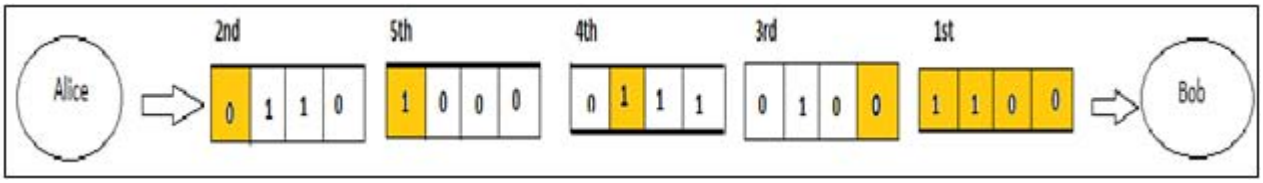


Figure 5: Transmitting of frames in unique order storing and transferring confidential data [7].

5. Future Work

The D-Scrabble physical layer security model is integrated with AI and the process has been humanized to offer unpredictability and evolution by NEAT technology. The working model will require a Scrabble game AI. The complexity of game AI and its game parameters will greatly determine the security level of D-Scrabble. A pattern matching algorithm and implementing cyclic technology are also to be considered. The relation of Network specifications and its requirements with the Scrabble game should be determined. The development of D- Scrabble model integrated with AI, comparing it with other models and examining its vulnerability towards various attacks is precisely the future work of this paper.

6. Conclusion

This model has many security layers to protect the individual from attacker. This model works at bit level and offers additional security to the existing models. Physical layer security has to work along with encryption algorithms to ensure more security in today‟s world where computational power of computers is ever-increasing. It also includes NEAT AI and integrates it with security by Scrabble game AI. A new cyclic technology is also devised. The approach of humanizing the security process is new and introduces high level of security.

References

[1] Retrieved from “https://en.wikipedia.org/wiki/Neuroevolution_of_augment ing_topologies”
[2] Kenneth O. Stanley, Risto Miikkulainen, “Evolving Neural Networks through Augmenting Topologies”, The MIT Press Journals, Evolutionary Computation Volume 10, Number 2.
[3] David Adrian Karthikeyan Bhargavan,”Imperfect Forward Secrecy:How Diffie-Hellman Fails in Practice”, 22nd ACM Conference on Computer and Communications Security (CCS ‟15), Denver, CO, October 2015.
[4] Martin Abadi *University of California at Santa Cru,* ‟Trusted Computing, Trusted Third Parties, and Verified Communications”, Security and Protection in Information Processing Systems Volume 147 of the series IFIP — The International Federation for Information Processing pp 291- 308.
[5] Amitav Mukherjee, *Member, IEEE,* S. Ali A.

Fakoorian, *Student Member, IEEE,* Jing Huang, *Member, IEEE,* and Lee Swindlehurst, *Fellow, IEEE,"* Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey", Published in IEEE Communications Surveys & Tutorials (Volume: 16 , Issue: 3).

[6] Aylin Yener, Fellow IEEE and Sennur Ulukus, Member IEEE, "Wireless Physical-Layer Security: Lessons Learned From Information Theory", Proceedings of the IEEE (Volume: 103, Issue: 10).

[7] James C. Peterson, "Method and system for encryption of file characteristics of .ZIP files" patent US7793099 Sep 20, 2004 Sep 7, 2010 Pkware, I

Author Profile

Devansh Dave is an undergraduate student from K.J.Somaiya CoE currently pursuing research in security with AI, Operating systems and Data mining. Mumbai, India.