Providing Wireless Network Security by Joint Physical Security and Signcryption Scheme

Nasser Ramazani[1], Hammid Reza Dalili Oskoei[1], Bahram Vazirnejhad[2]
[1]University of Aeronautical Science & Technology
Tehran, Iran
[2]Sharif University of technology
Tehran, Iran
nasser.rammazani @gmail.com, h_oskouei@yahoo.com, bahram@sharif.edu

ABSTRACT: *In a wireless network whatever try to isolate network against eavesdroppers but always there is a leakage probability of information. On the other hand considering the weaknesses of cryptography algorithms and attacks performed against them, cryptography alone cannot guarantee the security of communications in a wireless network. The goal of this paper is to gather solutions for creating a secure wireless network. With regard to the developments in wireless communication networks brought about by smart array antennas, security can be sought in the physical layer as well, aiming to restrict the access of the data in a wireless network and limit it to authorized users only in order to further restrain malicious data accesses. Furthermore, we analysis a strategy for restricting data access using smart array antennas and present the results in security by a parameter called exposure region. For this strategy afterwards we propose a new hybrid protocol for network security based on cryptography algorithms. This protocol allows users to authenticate the sender's identity taking advantage of signcryption schemes while exerting a negligible computational load on the network.*

Keywords: Smart Antennas, Signcryption, Physical Layer Security, Wireless Networks

Received: 7 July 2013, Revised 19 August 2013, Accepted 28 August 2013

1. Introducttion

With the growing prevalence of wireless communication networks, the security of the information being transferred in the network and preventing them from being revealed has become crucial. In wireless networks this is done through encryption schemes among which WEP is one of the most known. These methods hide the content of the information from attackers and use common encryption algorithms [1]. For example, WEP and WPA use RC4 stream cipher algorithm on which more effective attacks have been performed and WPA2 uses AES. The security of standard cryptographic algorithms is computational security therefore attackers cannot access the content of the data they have gained through eavesdropping of the messages if they test all possible solutions.

In a wireless network whatever try to isolate network against eavesdroppers, but always there is a leakage probability of information. The main question arising here is whether it is possible to prevent the attackers from eavesdrops the messages or not. This problem is known as the security of the physical layer and is aimed at taking measures in the communicational infrastructure to limit the possibility of sending and receiving information to authorized users only [2]. The solution to this problem is using smart antennas that have the ability to concentrate communicational information. These antennas can direct

the beam in the desired direction to limit the exposure region of the information and send them only to the areas belonging to authorized users. Therefore, the exposure region can be counted as a criterion for measuring security in the physical layer. This region is considered as an area in which attackers can access the information and it has been shown that by increasing the elements of the array antenna, exposure region will be limited and therefore the attacker chance for eavesdropping decreases. We will show, this strategy called Aegis [3], alone will not be enough to provide security in the network. Thus, we try to provide an appropriate protocol using cryptography techniques with low computation complexity inside of considering security in physical layer.

Block cipher algorithms are used in different modes including AON (All-or-Nothing) transforms proposed by Rivest [4]. In this method, accessing the content of one packet requires the decryption of all the packets. We analyze the Aegis method and show disadvantages of this strategy and then we will show by manipulating of AON and cryptographic schemes we can provide a secure network. To solve the problem of key transfer between the users and the network and also to secure network against actives attackers, an improved version of signcryption is used [5]. This algorithm reduces the computational load imposed on the network. Considering that cryptography protocols should be immune against known attacks it is necessary to analyze the protocol from this point of view. Obviously, by gathering all solutions for creating a high level secure wireless network we can minimize leakage probability of information.

In this paper, we discuss about advantages in security caused using smart antennas and then propose a secure hybrid protocol to joint security in physical layer and a higher level layer. Finally, after security analysis of the protocol we improve it by exploiting a signcryption scheme which is an efficient cryptographic scheme supporting digital signature and encryption together.

2. The security scheme based on AON method

The basic assumption here is that each user can access multiple access points. Thus by transferring only one part of the data with each access point, accessing the data will become harder for attackers since the attackers are then forced to enter the region shared by all the access point to be able to get all of the data. This idea can use time, space and frequency as different dimensions for splitting the data. Here we focus on space which is accomplished through a virtual array [2]. This technique is based on sending different parts of the data through distinct paths where each part of the data needs decryption.

Consider a secure pseudo-random generator that uses a private key K for producing the pseudo-random sequence PRNG (K). Assume that the message being sent is a bit sequence with the length $|M|$. This sequence undergoes an XOR operation with the bit sequence generated by PRNG (K) to produce the ciphertext C with the length $|C|$ which is similar to the message $|M|$. This cipher text is divided into a number of $|K|$ bit blocks. Each of these blocks undergo an XOR operation first with each other and then with the key K and the result will be named C_L. Now the network controller divides the new message $C \| CL$ into $|K|$ bit segments. All these segments should be delivered to the receiver completely. When the receiver receives all these segments completely, performs an XOR operation on all of them to get the key K. When K is achieved, the receiver uses it for decrypting the segments and then sorts them according to segment number to reconstruct the message. On the other hand, the eavesdropper who is located in the path between the first access point and the user will be able to get the first segment of the data only. If he desires to access the other parts of the data, he should move to the path of another access point in a time faster than one time interval, which is impossible or being in exposure region.

3. Using smart array antennas to provide physical layer security

An easy way for reducing the chances of eavesdropping is using beamforming; the signal will be enclosed in a specific region between the sender and the receiver which is dependent upon the shape and the domain of the beam pattern and the channel.

This characteristic of smart array antennas is so useful for providing security in wireless networks. Now we will compare smart antennas against omni-directional antennas and use a valid approximate geometric model for the shape of the beam. In this scenario, an attacker is present in the exposure region of the access points. In the next section we will perform the analysis and show how a beamforming mechanism improves security in comparison with an omni-directional antenna. For reaching this goal we calculate the exposure region in each case using geometric modeling based [3], also for calculating the security advantages and comparing the exposure region, we need to find out the area of the exposure region in the omni-directional case and array antennas case.

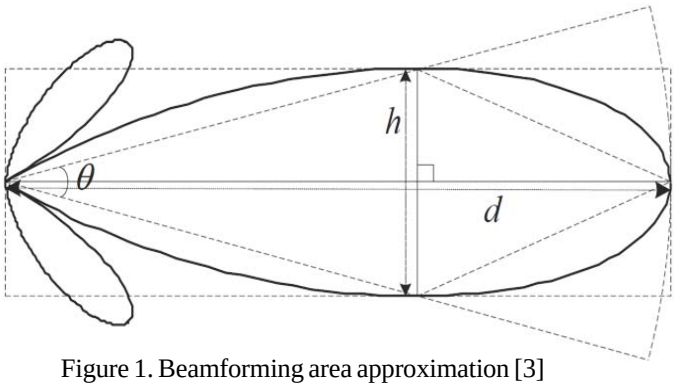

Figure 1. Beamforming area approximation [3]

3.1 Geometric analysis

Here we use two types of approximation, *inscribed parallelogram* and *sector* models as shown in Fig1. We use both of these approximations for comparison exposure region. The shared region *S* is the region of access, meaning that the receiver will be able to access the whole data only in this region. By [3] for a smart array antenna using *k* elements, distance between client and AP which is showed with *d* could be defined as

$$d = \left(\frac{P_t G_t G_r \lambda^2}{4\pi \times P_{th}}\right)^{1/\alpha} \tag{1}$$

G_r and G_t are main gain lobe of receive and transmit that assume to be 1. P_{th} denotes power threshold and P_t denotes transmitting power also α and λ means path loss exponent and wavelength.

The area can be calculated using the *sector* model as below:

$$A_2 = \frac{1}{2} d^2 \theta \tag{2}$$

Where θ is the null-null beam width of the transmitting or receive antenna. For a linear array with *k* elements and a uniform excitation, it is given by

$$\theta = 2\sin^{-1}\left(\frac{2}{k}\right) \tag{3}$$

As a function of *k*, the distance can be written this way:

$$d = c_1 k^{1/\alpha} \tag{4}$$

Here, $c_1 = \left(\frac{P_t \lambda^2}{4\pi P_{th}}\right)^{1/\alpha}$ and therefore the approximate area of sector A_2 is given as below:

$$A_2 = 2c_1^2 k^{2/\alpha} \sin^{-1}\left(\frac{2}{k}\right) \tag{5}$$

On the other hand, for the area of the omni-directional antenna we will have:

$$A_1 = \pi d^2 \rightarrow A_1 = \pi c_1^2 \tag{6}$$

Now if we find out the proportion of the two areas $\frac{A_2}{A_1}$ we can compare the proportion of the exposure region for the smart antenna

$$\frac{A_2}{A_1} = \frac{2}{\pi} k^{2/\alpha} \sin^{-1}\left(\frac{2}{\alpha}\right) \tag{7}$$

For more comprehending in Figure 2 we show the behavior of this proportion. The values for the proportion are given for α equal to 2, 3, and 4. Evidently with the increase of the element *k*, the pattern of the antenna and the region of exposure become smaller. Therefore, by limiting the region for the user through the increase of *k*, the hacker's access to the data will be restricted.

Additionally, the path loss exponent affects the region of exposure as well. Overall, the reduction in the region of exposure is less than linear.

The above results show that with the change of *k* we can gain security advantages with the simple form beam. Even though the beam form is a mechanism for increasing security, but the question is whether it is possible to achieve greater advantages using more APs.

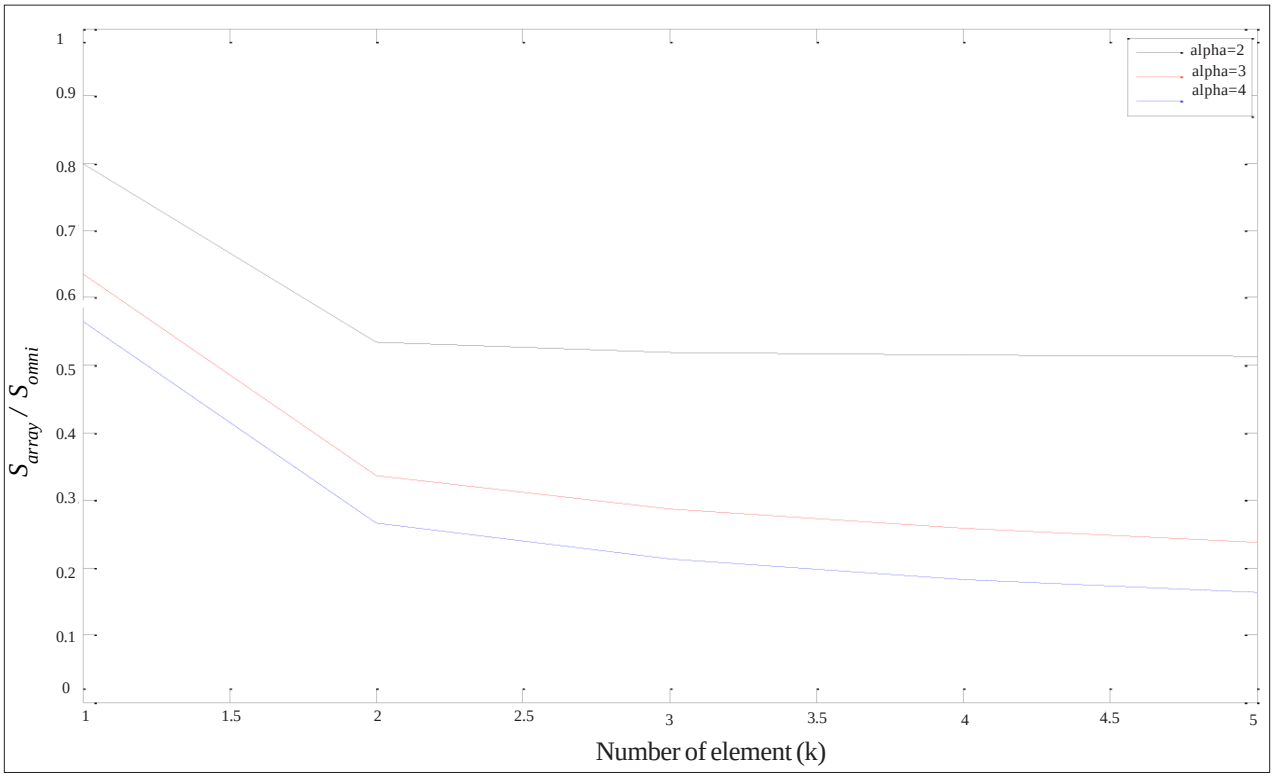

Figure 2. Proportion of the two areas A_2 / A_1

3.2 Increasing advantages of security using multiple access points

In this case we assume to have 4 access points and we try to calculate the exposure region for the 4 access points for the omni-directional antenna and the array antenna cases. Obviously the presence of 4 access points in the general case makes the geometric space asymmetrical and therefore estimating the shared exposure region for 4 patterns will not be easy. For simplifying the problem, we consider the case where the 4 access points are located on the four corners of a square. If we have 4 similar access points on the four corners of a square the exposure region will be the area shared by the areas of the four access points. Attackers are then able to access the data only in the region shared by the APs patterns. This is shown more clearly in Figure 3.

Now suppose *X* to be the distance between the two access points. To calculate the region of exposure, we should go through the following geometric calculations in order to express the area of *S* in terms of *d* and *X*.

Considering geometric formulas; it can easily be shown that the angle null to null beam width θ can be calculated as below:

$$\frac{\pi}{4} - \sin^{-1}\left(\frac{X}{2d}\right) = \theta \tag{8}$$

Having θ in Figure 3, we can easily find out the area of the hatched region by first finding the area of the sector and then adding it to the area of the region formed by the intersection of the arcs. The area of a section of the circle created by the angle 2θ is as follows: The area of the extra part of the Arc = area of the Arc FP_1E – area of the triangle FP_1E

$$S_1 = \frac{1}{2} d^2 (2\theta) - \frac{1}{2} d^2 \sin(2\theta) \tag{9}$$

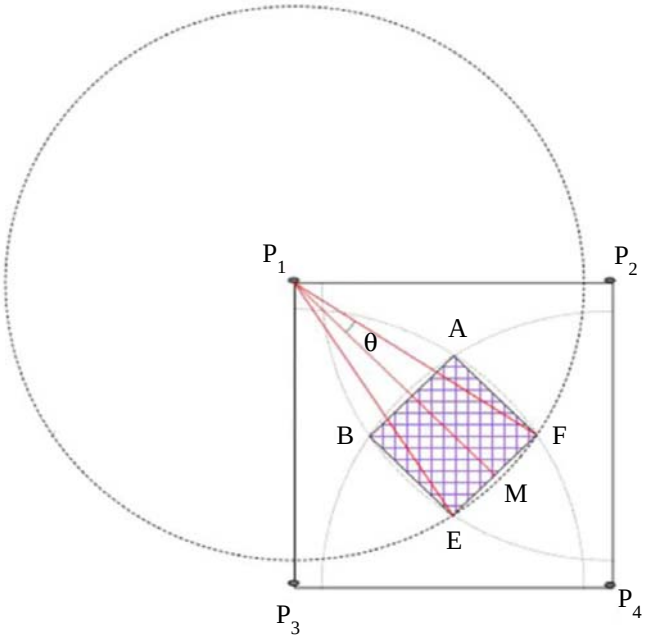

Figure 3. Exposure region approximation of 4 APs using omni directional antenna

The area of the square ABEF is given below:

$$S_2 = (2 \mid \overline{FM} \mid)^2 = 4\,(d \sin \theta)^2 = 4d^2 \sin^2 \theta \tag{10}$$

Therefore total region could be achieved by this formula:

$$S_{omni} = S_2 + 4S_1 \tag{11}$$

$$S_{omni} = 4d^2 \sin^2 \theta + 4d^2 \theta - 2d^2 \sin^2 (2\theta) \tag{12}$$

Now we assume that an array antenna is used instead of a normal antenna (We assume that the pattern form of all of the antennas

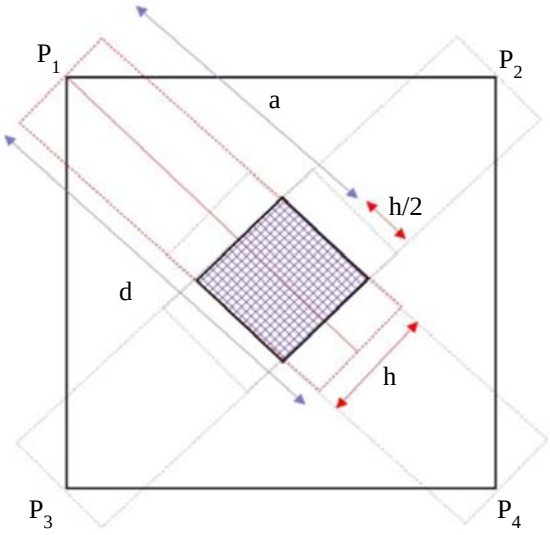

Figure 4. Exposure region approximation of 4 APs using smart antennas

are rectangular). We then calculate the area in proportion to the last case.

Here we use inscribed parallelogram model for area approximation of each access point. According to Figure 4 and assuming that $d - a > h / 2$ the area will be as follows:

$$S_{array} = h^2 \tag{13}$$

Therefore, the proportion of the areas will be as follows:

$$\frac{S_{array}}{S_{omni}} = \frac{4k^{\frac{2}{\alpha}} \times (\sin^{-1}(\frac{2}{k}))^2}{16\sin^2\theta + 4\theta - 2\sin(2\theta)} \tag{14}$$

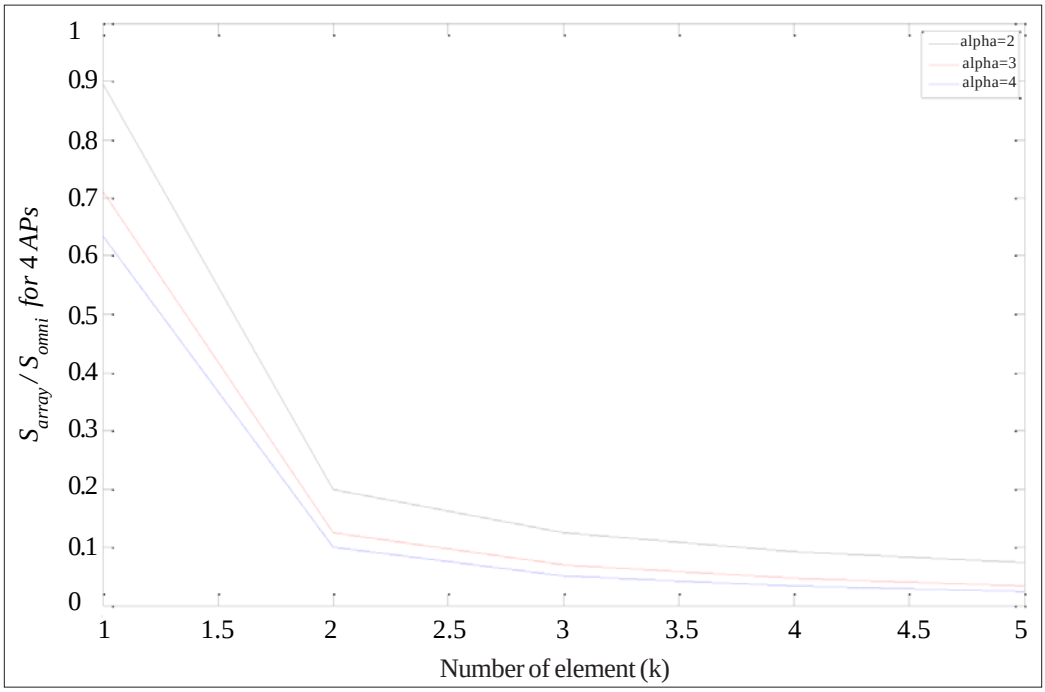

Figure 5. The proportion of exposure region Sarray/Somni using 4 access points when we have smart array antenna or omni-directional antenna, we assume X/d = 1

As we could see in Figure 5 by growing smart antenna elements k the exposure region would be decreased. Therefore when using multiple access points, the proportion decreases drastically with the increase in the number of elements k. This is a good idea to limit accessing of attacker from information that is based on Aegis. By using the other properties of smart antenna we could use some technics like jamming but the use of such technics reduces network throughput. However when a client has access to multiple APs the controller can divide information and send them by multiple sender. But this method should be used in correct manner unless there is the risk of key leakage. We show this problem at the next section.

4. Security problems, disadvantages and improving the Aegis physical layer security scheme

The main flaw in this scheme is that attackers by locating in exposure region can still easily access and decrypt all of the data if they find all of the segments of the encrypted text by performing an XOR operation on the segments and finding the key. Assume an eavesdropper gain information being transmitted $C' = C \,||\, C_L$. All of work he must do is to divide C' into $|K|$ bit blocks (since the length of key is public) then XOR all parts together and achieve the private key K. Therefore, Aegis scheme only limit attackers to gain information and does not bring about security.

As it was observed, even the techniques was presented for the security of the physical layer called Aegis can not prevent attackers from accessing the data and they can still lay hands on the main data with a considerable probability. Therefore, here

Algorithm1*: Encrypting message in sender*

INPUT: *m, PK*, random key *K*

OUTPUT: Encrypted message *C*

1) Divide message *m* to | *K* | bit segments. Use concatenate scheme if it is needed.
2) Encrypt all message segments m_i by symmetric algorithm such that

$c_i = e_K(m_i),\ 1 \le i \le s$

3) Encrypt random key *K* by public key algorithm

$c'_K = E_{PK}(K)$

4) XOR all encrypted message segments together with encrypted random key c'_K

$c'' = c_K \oplus c_1 \oplus c_1 \oplus \ldots \oplus c_s$

5) Concatenate c'' and all c_i , then send *C* to client.

$C = c'' \| c_i,\ 1 \le i \le s$

Algorithm1*: Decrypting message in receiver*

INPUT: *C, SK*

OUTPUT: Decrypted message *m*

1) Divide *C* to | *K* | bit segments.
2) XOR all encrypted message segments together to earn encrypted random key.

$c'_K = c'' \oplus c_1 \oplus c_1 \oplus \ldots \oplus c_s$

3) Decrypt random key c'_K by public key algorithm

$K = D_{SK}(c'_K)$

4) Decrypt all segments by random key *K*.

$m_i = d_k(c_i),\ 1 \le i \le s$

we design a protocol that in addition to limiting the chance of eavesdropping provides adequate security against effective attacks by using physical layer security techniques as well as public key encryption methods. We denote the public key P_K then E_{PK} shows an asymmetric encryption algorithm. Also we use S_K to denote receiver private key and D_{Sk} to show asymmetric decryption algorithm, correspondingly. Using e_K and d_K we show symmetric encryption and decryption algorithms an here *K* denotes private random key. Asymmetric algorithms are suitable and secure for encrypting information but because of their computation complexities we must be careful when using them. In a communication networks there are a lot of clients which network responds to them; therefore we can not burden a lot of computation to it. For having least computation and most security we encrypt each of segments with a secure symmetric encryption algorithm which has low computation complexity and uses a private random key, then we exploit a secure asymmetric encryption algorithm for encrypting private random key.

Consider m to be the message being sent. The proposed protocol is shown in algorithm1. In this manner if an attacker gather all segments $C = C'' \| C_i$ and XOR all of them would obtain C_K encrypted random key and can not doing decryption. Transmitting segments equal to number of access points in each transmission order could divide information in which the attacker have no chance to earn all of segments. In other words, considering s as number of APs each client is having access to them therefore by use of this protocol at any transmitting duration just s segment could be sent, therefore it is impossible for an attacker to gather all of segments. Also if he gathers all segments could not decrypt them because of using public key cryptosystem.

5. Security Analysis

Since cryptographic techniques have been used for providing security, we will with security based on the two separate scenarios of active and passive attackers in the remainder of this paper. In other words, the level of security needed for the two protocols will be discussed with regard to the abilities of the attackers.

5.1 Passive attackers

An attacker who just can eavesdrop the transmission data and can not impress them called passive attacker .Here, we assume that the attackers have the ability to breach into the shared region, or there are multiple collaborating attackers who are located in the patterns of all of the access points and can get all of the encrypted data segments. In other words, we are assuming here that attackers possess all of the encrypted packets and the following security should be taken into consideration.

5.1.1 Security against known plain text attacks

In these attacks, hackers possess a part of the plain text as well as the encrypted text [6]. As it was observed, in each transfer one

random key *K* can be selected to encrypt the data. This in fact provides forward secrecy [7], meaning that since one *K* is selected in each transfer, the disclosure of the key *K* in one round does not threat the security of the whole transfer because *K* will change in the next transfer. Additionally, if the hackers try to access the main key while possessing only a number of the blocks of the encrypted text and the plaintext, they need to be able to break the symmetric encryption used in the algorithm, and by using secure symmetric encryption algorithms we make it impossible for them to do so.

5.1.2 Security against known ciphertext attacks In this attack, hackers need to access parts of the data while possessing the encrypted text. Brute force attacks are the most common type of these attacks against which we have protected our system using the AON method [4]. It must be noted that to stop such hackers all that needs to be done is to use symmetric and asymmetric encryption systems which are immune against these attacks. Encrypt Symmetric stream ciphers and also AES [8] block cipher enjoys this level of security. Additionally, with the use of asymmetric encryption methods which are immune against such attacks, this level of security can be guaranteed. Overall, it can be said that this protocol is secure against known encrypted text attacks through using standard encryption algorithms.

5.1.3 Security against selected encrypted text attacks
In this scenario, hackers can select parts of the encrypted text, find out the corresponding plain text, and use this information to find the main key or other parts of the encrypted text. This attack and its equivalent, comparative selected encrypted text attack, are the most powerful attacks against public key encryption systems. In this protocol, the randomly generated key is encrypted using the public key system and therefore the public key system must be immune against this attack. RSA encryption system is not immune against this attack, although the RSA-OAEP scheme can be used to solve this problem since this system is secure against selected encrypted text attacks.

5.2 Active attackers
So far, we discussed network security against eavesdropper and we showed that by using security techniques in the physical layer and the higher level layer we can reach this level of security. Now the question is that if the attackers impersonate the network and produce patterns for the users and send information to them, how can the user decide this information is not sent by authorized access points? Unfortunately, this protocol is not secure against this type of active attackers who can intrude and affect the network. The most suitable solution against these attacks is the use of digital signatures by the sender, meaning that the network allows the receiver to authenticate the sender of the packets by providing signatures for the packets and sending them alongside the packets. Therefore, only the messages whose signatures are confirmed by the receiver are considered valid. Unfortunately, utilizing these public key algorithms imposes a high amount of computational load on the sender and also adds overload to the packets. Therefore, selecting the proper protocol here is crucial. A very suitable algorithm here is signcryption which serves as an encryption and a signature solution at the same time. Signcryption was first introduced by Zheng [9] and its different features have been analyzed henceforth. The original scheme provides confidentiality and unforgeability for the message but cannot guarantee non-repudiation and forward secrecy. However, these features have been added to this algorithm in the scheme presented by [5]. Here, we utilize this scheme with a little modification which does guarantee non-repudiation and by using random keys, we make the network secure enough for transferring keys and prevent attackers from sending fake messages to the users. Additionally, to reduce the computational load of the network, we have tried to move the load to the user by avoiding the use of inverse element when signing the messages in the signcryption algorithm. In comparison with other variations of the signcryption protocol, the version based on the DL problem has very low power transmit cost. By implementing exponential in module based on Shamir's algorithm [9], this cost can become as low as 1.17 exponential.

6. The proposed protocol for security against active attackers

The signcryption algorithm has a lot of varieties but for having the best performance on the network we must consider some modifications. We do some modifications on signcryption algorithm for having low complexity load. We can now define a protocol for the network based on this scheme which secures information transfer in the physical layer and the higher level layer in a way that prevents eavesdroppers from accessing the plaintext even after accessing the transferred information. Additionally, active attackers will not be able to send fake messages to the users. Here, it has been assumed that a CA center has given certificates to each of the clients. In addition to that, the network uses controllers to schedule the transfer of the packets and their sequence.

Assume p to be a large prime number and q to be a large prime number factor of $p-1$. Furthermore, assume g to be an integer of order q modulo p which is selected from Zp^*. (E, D) are the symmetric encryption and decryption algorithms. x_a is the private key

of the sender, $y_a = g^{x_a} \bmod p$ will be the public key of the sender, also x_b is the private key of the receiver and y_b will be its corresponding public key and G is a secure hash function. Before transmission the network controller must do these tasks:

i) *First, all of the users in the network and the number of access points are found out.*

ii) *The number of access points for each user and the number of users for each access point are reviewed.*

Now consider that the number of access points assigned to the i_{th} user is n. Then regarding the length of the selected symmetric encryption key $|K_{session}|$, we take out n packets of the length $|K_{session}|$. If the length of the total information being sent is L bits, $n \times |K_{session}|$ bits will be sent in each transfer (Here we have assumed that $L \geq n \times |K_{session}|$).

Afterwards, the server signs the message using the improved signcryption algorithm and encrypts the key of the session in the following way.

Algorithm 2: *Signcrypting message in sender*

INPUT: $m, K_{session}, y_b, x_a, t$

OUTPUT: c, r, s

1) $ci = E_{K_{session}}(m_i), 1 \leq i \leq n$

2) $c = c_1 \| c_1 \| ... \| c_n$

3) $M = K_{session} \| G(c, K_{session})$

4) $e = G((y_b^t \bmod p), c)$

5) $r = M \oplus e, s = (t - x_a r) \bmod q$

Algorithm 2*: Decrypting and verifying message in receiver*

INPUT: c, r, s, x_b, y_a

OUTPUT: m

1) $e = G(y_b^s . y_a^{x_b . r} \bmod p, c)$

2) $M = e \oplus r \rightarrow M = K'_{session} \| G(c, K_{session})$

Verify $G(c, K'_{session}) = G(c, K_{session})$

3) $m_i = D_{K'_{session}}(m_i), 1 \leq i \leq n$

According to $t \in Z_q^*$, is a random parameter chosen by the server. For simplifying the protocol, the encryption part of the signcryption algorithm has been omitted. Also assume $K_{session}$ to be the random key selected by the sender in each transmitting session. The messages m_i are encrypted using this key and exploiting the selected symmetric encryption algorithm.

Now the packets c_i should be sent to the receiver along with r and s. Each packet is sent using one access point to keep the physical layer secure and prevent attackers from accessing all of the packets together. After receiving the packets, the user can validate and decrypt the message using his private key *xb* in the following way. r and s can be concatenated to sequences of prefix zeros to reach the length $|m_i|$.

Here, the scheme of the signature has changed from $s = t(r + x_a)^{-1} \bmod q$ $s = t - rx_a$) to move the computational load to the receiver's side. In this scheme, only the sender can perform the signature operation because x_a is confidential and therefore unforgeability has been guaranteed. The confidentiality of the message has also been guaranteed using the symmetric encryption. Additionally, the presence of the private key x_b means that only the receiver can make a secret parameter e and validate and decrypt the message. It is assumed that DL is an unsolvable problem and G is a secure hash function.

6.1 Advantages of proposed protocol

Generally, we could claim this protocol involves security in the physical layer and the higher level layer, in other words not only we provided security by cryptographic consideration but also drastically, decreased attackers opportunity for eavesdropping the transmission information by using smart antenna in an appropriate way. We sort these advantages here:

1) *Minimum opportunity for eavesdropping*. Transmitting segments equal to number of access points in each transmission session could divide information, in which attackers have a little chance to earn all of segments.

2) *Using smart antenna minimizes the exposure region*. Therefore, the chance of eavesdropping proportionally decreases.

3) *Signcryption schemes provide benefits of digital signature and encryption with low costs of complexity.* Exploiting this algorithm immunizes networks against active attackers in which nobody except the rightful authority could send information to

a client.

The importance of signcryption in security against important attacks like chosen ciphertext attacks is discussed thoroughly in [10]. We have therefore not only made information transfer in the network possible using encryption, but also provided physical layer security for the network. The network will even be able to use jamming control and stream overwhelming techniques [3] but these techniques, however, will not be cost effective because of the high costs they impose on the network and negative influences in the network throughput. Using signcryption, we were eventually able to prevent attacks by active attackers. In the design of this protocol, we have tried to use the most up-to-date public key algorithms with high security and low costs, especially the signcryption algorithm which needs a mere 1.17 transmit power for validation which is the lowest number among same protocols. Additionally, the lowest amount of overhead will be added to the transferred data [9]. The use of private keys in the receiver's side guarantees that only the receiver can validate and decrypt the private session key in each transmission session. These keys add forward secrecy to the system so that if attackers get access to the key of one round data transfer will not be threatened since this key will change.

7. Conclusion

The most important security issue is preventing attackers from accessing the data being transferred, even in encrypted form. In wireless networks, omni-directional antennas do not allow this because they broadcast the data in the region and attackers can easily access the data being sent.

As we know by using smart array antennas we can limit the region of exposure of the data. On the other hand, it was shown that we cannot rely on these antennas alone for securing the network and consequently we added a public key encryption system to our method to build a complete network security protocol. In this stage, security analysis on the protocol showed that active attackers can still threaten the network and finally we showed that using signcryption, we can not only prevent malicious data accesses, but also add new security features to the system including forward secrecy and non-repudiation.

References

[1] Beck, M., Tews, E. (2009). Practical attacks against WEP and WPA. *In*: Proceedings WISEC 09, p. 79-86, USA.

[2] Lakshmanan, S., Tsao, C. L., Sivakumar, R., Sundaresan, K. (2008). Securing Wireless Data Networks against Eavesdropping using Smart Antennas. *In*: Proceedings ICDCS, p. 19-27.

[3] Lakshmanan, S. (2010). Aegis: Physical Space Security for Wireless Networks With Smart Antennas. *IEEE Transactions on Networking*, 18 (4) 1105-1118.

[4] Rivest, R. (1997). All-or-nothing encryption and the package transform. *In*: Proceeding Fast Software Encryption, p. 210–218.

[5] Ho, W. H. (1999). Cryptanalysis and improvement of Petersen-Michels. *In*: Proceeding IEE Computers and Digital Techniques, p. 123-124.

[6] Stallings, W. (2005). Cryptography and Network Security. Prentice Hall.

[7] Miner, S., Bellare, M.(1999). A forward-secure digital signature scheme. LNCS, Lecture Notes in Computer Science, 1666.

[8] Announcing the Advanced Encryption Standard (AES). (2001). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST).

[9] Zheng, Y. (1997). Digital signcryption or how to achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption). LNCS, Lecture Notes in Computer Science , 1294, p 165-179,.

[10] Baek, J., Steinfeld, R., Zheng, Y. (2002). Formal Proofs for the Security of Signcryption. *In*: Proceeding PKC '02 Proceedings of the 5th International Workshop on Practice and Theory in Public Key Cryptosystems: Public Key Cryptography, p. 80-98.