Proposing a Hybrid Protocol for Secure Wireless Networks based on Signcryption scheme

Nasser Ramazani Darmian
University of Aeronautical Science & Technology
Tehran, Iran
Nasser.rammazani@gmail.com

H.R. Dalili Oskoei
University of Aeronautical Science & Technology
Tehran, Iran
h_oskouei@yahoo.com

B.Vazirnejhad
Sharif University of technology
Tehran, Iran
bahram@sharif.edu

Abstract—considering the weaknesses of cryptography algorithms and the attacks performed against them, cryptography alone cannot guarantee the security of communication in a 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. In this paper, 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-component; Array antennas, Signcryption, Physical layer security, Beam forming;

I. INTRODUCTION

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. 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 cryptography algorithms is computational security, i.e. attackers cannot access the content of the data they have gained through eavesdropping of the messages. 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 pattern. 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, the 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 for securing the network. Thus, we have tried to provide an appropriate protocol using cryptography techniques with low computation complexity.

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. In this paper first we analyze the Aegis method and show disadvantages of this strategy, then we will show by manipulating of AON and cryptography 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 reduce 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.

II. 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 an $L$ bit long private key $K$ for producing the pseudo-random sequence $\text{PRNG}(K)$. 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 $\text{PRNG}(K)$ to produce the ciphertext $C$ with the length $|C|$ which is similar to the message $M$. This ciphertext 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 $C||C_L$ into $|K|$ bit segments. All these segments should be delivered to the receiver completely. When the receiver receives all these segments completely, she 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 packet. 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.

With the application of this mechanism, attackers need to be in the region shared by the multiple access points to have access all of the data.

III. USING 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.

Now we will compare smart antennas against omnidirectional 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 one of the access points. In the next section we will perform the analysis and show how a beamforming mechanism improves security in comparison with a multi-directional antenna. For reaching this goal we calculate the exposure region in each case using geometric modeling based [3]. With the application of this mechanism, attackers need to be in the region shared by the multiple access points to have access all of the data and as it can be seen in Fig1 for four access points, the exposure region decreases when smart antennas are used and the security increases in the physical layer. 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. For comparison, we calculate the exposure region for the cases of 4 access points.

Region of exposure when using 4 access points: In this case we assume to have 4 access point and we try to calculate the exposure region for the 4 access points for the simple 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 region of exposure 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 receiver patterns. This is shown more clearly in Fig1.

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. Now suppose $X$ to be the distance between the two access points, as Fig1.a shows. 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 $X$. By [3] for a smart array antenna using $k$ elements, $d$ could be defined as

$$d = \frac{P_G G_d A^2}{4\pi \times P_h}$$

Considering geometric formulas; it can easily be shown that the angle $\theta$ can be calculated as below:

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

Having $\theta$, 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 $2\theta$ is as follows: The area of the extra part of the Arc = area of the Arc $FP_EE -$ area of the triangle $FP_EE$

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

The area of the square $ABEF$ is given below:

$$S_2 = (2FM)^2 = 4(d \sin \theta)^2 = 4d^2 \sin^2 \theta$$

$$S_{\text{omni}} = S_1 + 4S_1$$

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

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 are rectangular). We then calculate the area in proportion to the last case. According to Fig.1-b and assuming that $d-a > h/2$ the area will be as follows:

$$S_{\text{array}} = h^2$$

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

$$\frac{S_{\text{array}}}{S_{\text{omni}}} = \frac{4k^2 \times (\sin^{-1}(\frac{2}{k}))^2}{16\sin^2 \theta + 4\theta - 2\sin(2\theta)}$$
Fig. 2 shows the proportion of the exposure region when using array antennas to the region of exposure when using omni-directional antennas.

As we could see in Fig. 2 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.

IV. 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. 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 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 $PK$ and $E_{PK}$ shows the asymmetric encryption algorithm. Also we use $SK$ to denote receiver private key. Symmetric algorithms are suitable and secure for encrypting information but because of their computation complexities we must be careful for using them. In a communication networks there are a lot of clients that 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 by a secure symmetric encryption algorithm which has low computation complexity and use a secure asymmetric encryption algorithm for private key must be transmitted. In this manner if an attacker earn $C''=C||C_k$ and XOR all of them would obtain $C_k$ encrypted random key and can not doing decryption.
Consider $m$ to be the message being sent. The proposed protocol is as follows:

### Security Protocol 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
   
   $$c_i = e_K(m_i), \ 1 \leq i \leq s$$
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 $K$
   
   $$c'' = c'_K \oplus c_1 \oplus c_2 \oplus \ldots \oplus c_s.$$ 
5. Concatenate $c''$ and all $c_i$, then send $C$ to client.

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

### Security Protocol in Receiver

**INPUT:** $C$, $SK$  
**OUTPUT:** $m$

1. Divide $C$ to $|K|$ bit segments.
2. XOR all encrypted message segments together to earn encrypted random key.
   
   $$c'_K = c'' \oplus c_1 \oplus c_2 \oplus \ldots \oplus c_s.$$ 
3. Decrypt random key $K$ by public key algorithm
   
   $$K = D_{SK}(c'_K).$$
4. Decrypt all segments by random key $K$.

   $$m_i = e_K(c_j), \ 1 \leq i \leq s.$$

V. 4. SECURITY ANALYSIS

Since multiple techniques have been used for providing security, we will deal 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.

### A. 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.

For defiance against this types of attacks we should use secure cryptography algorithms like AES [6]. Through progression in cryptography, by use of standard algorithm if such attackers could achieve transmission information by eavesdropping, would not able to detect true meaning of information [7]. Overall, it can be said that this protocol is secure against passive attackers through using standard encryption algorithms. Additionally, in each transfer one random key $K$ can be selected to encrypt the information. This in fact provides forward secrecy [8], 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.

### B. Active attackers

So far, we discussed network security against eavesdropper and we showed that by using security techniques in the physical layer and the user level 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 receiver 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 the least power transmit cost. By implementing discrete logarithm power transmission based on Shamir’s algorithm [9], this cost can become as low as 1.17 exponential.

VI. THE PROPOSED PROTOCOL FOR SECURITY AGAINST ACTIVE ATTACKERS

The signcryption algorithm can be used as follows. It is assumed that DL is an unsolvable problem and $G$ is a secure hash function. We also do some modifications on signcryption algorithm for having low complexity load.

Assume $p$ to be a large prime number and $q$ to be a large prime number factor of $p-1$. Additionally, assume $g$ to be an integer of order $q$ modulo $p$, which is randomly selected from $Z^*_p$, $(E, D)$ will be the symmetric encryption and decryption algorithms. $x_a$ will be the private key of the sender, $y_a = g^{*} mod p$ will be the public key of the sender, $x_a$ will be the private key of the receiver, and $y_b$ will be its corresponding public key.

Here, the scheme of the signature has changed from $s = (r+x_a) \text{ mod } q$ to $s = (t-x_a) \text{ mod } q$ 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 $x_a$ means that only the receiver can make the parameter $e$ and validate and decrypt the message. The XOR between $K$ and $e$ is to make sure that $r$ and other outgoing messages have the same length.

We can now define a scheme for the network based on this protocol which secures information transfer in the application layer and the physical 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 each client a set of public key certificates to each of the clients. In addition to that, the network uses controllers to schedule the transfer of the packets and their sequence.

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 $n$-overhead packets of the length $|K_{session}|$. If the length of the total information being sent is $L$ bits, $n|K_{session}|$ bits will be sent in each transfer (Here we have assumed that $L > n|K_{session}|$).

Afterwards, the server signs the message using the improved signcryption algorithm and encrypts the key of the round in the following way. Take $x_a \in Z^*_p$ as the server’s private key and $y_a$ as the corresponding public key. Additionally, take $x_b \in Z^*_q$ to be the private key of the receiver and $y_b$ to be the corresponding public key. Here, $t \in Z^*_q$ is a random parameter chosen by the server. $p$ is a large prime number and $q$ is its divisor. For simplifying the protocol, the encryption part of the signcryption algorithm has been omitted. The modified version will now be explained. Assume $K_{session}$ to be the random key selected by the sender in each round. The messages $m_i$ which are usually at most 256 bits long is encrypted using this key using the selected encryption algorithm.

Therefore, if, $K_{session} \in Z^*_q$, then we have:

![Hybrid Protocol based signcryption in Sender]

![Hybrid Protocol based signcryption in Sender]

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 $x_i$ in the following way. $r$ and $s$ can be concatenated to sequences of prefix zeros to reach the length $|m_i|$. 
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. 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 keys in each round. 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.

VII. 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