Wireless security by handling computations

Sachin G.Chawhan, Dr.M.B.Chandak , Prof.Gurudev Sawarkar
Computer Science & Engineering, R.T. M.N.U. Nagpur
sachinchawhan11@gmail.com ; sawarkar92@gmail.com

Abstract—
Research on security in the domain of wireless has an active area. Wireless security study uses cryptographic tools. The major problem with these tolls, they based on computational assumptions, which may not be usable in the future. Hence there is requirement to make tools which are not dependable on assumptions. There is a tool known as 1-out-of-2 oblivious transfer tool which plays a major role in cryptography & can build a cryptographic protocol for any polynomial-time computable function which does not depend on any computational assumption. Privacy preserving password verification and private communication are applications. This protocol fully implemented on wireless devices and conducted experiments in real environments.

I. INTRODUCTION

Wireless domain has been an active area of research since the last decade. Generally to provide the security in wireless area an encryption, authentication & the key agreement are essential. These cryptographic tools are really good for use but a common weakness they have, they are based on computational assumptions. For example, symmetric key encryption. The other encryption schemes, e.g. ,AES. However, when we use AES to encrypt a message, it can be an implicit assumption: the AES block cipher is a pseudorandom permutation. Due to the above assumption of pseudo randomness which is based on the cryptologists understanding of the *current* attacks on encryption schemes. In the future it may possible, the AES scheme will be broken by newly invented cryptanalysis techniques. Some of the famous hash functions, including MD5 and SHA-0 work as a collision-resistant but cryptologists found that these assumptions are invalid. It will be necessary if we can remove cryptographic tools' dependence on such computational assumptions. It's a challenging problem to remove the computational assumptions form these tools. Here we are going to use wireless channel characteristics which used to build the cryptographic tool. These wireless channel characteristics are used to develop a tool known as 1-out-of-2 oblivious transfer. For simplicity it is known as OT (Oblivious transfer). Using OT one can use cryptographic protocol for any polynomial time computable function. The other protocols that can build using OT are electronic voting protocol, digital cash protocols etc. So using a this protocol we can build other protocols which will be independent of computational assumptions.

Both communicating devices share a Common secret key to communicate with each other privately. It can be observed that the security of such type of protocol based depend on the wireless channel characteristics, not on computational assumptions. The OT can be use as a protocol for privacy preserving password verification. In this method first communicating wireless device can verify a password from another communicating wireless device in such a way that the password is not known to either the first communicating wireless device nor by any attacker. In this paper the following major points highlighted.

• The main objective is to develop an OT protocol which is
depend on the physical characteristics. This protocol does not
depend on any computational assumption. It is a crucial step

to build a strong wireless system security & without using
computational assumptions.

• By using this protocol we can provide a private
communications and a technique of privacy preserving
password verification.

II. RELATED WORK

This tool is basically used to construct complex cryptographic protocols. Rabin was the first who proposed this tool first time. After some other people like Lempel, Even, Goldreich has propose OT, an important variant of OT. The main advantage of OT is its completeness. Any two party protocol can be built by using OT shown by Kilian and due to this result it can more beneficial by using it in case to construct multiparty protocols. Kilian and Cr´epeau present OT protocol which is based on noisy channels. To increase the efficiency Cr´epeau also proposed another OT protocol. Here the noisy channels they used are simple discrete memory less channels. In this approach we will use OT protocol which is based on wireless channels characteristics and which has more efficiency. We have demonstrated two applications of our OT21 protocol, private communications and privacy preserving password verification. In fact, there have been a number of works on private communications using the secrecy capacities of the wireless channel, among others. In particular, Vasudevantry to defend against the eavesdroppers by sending artificial noises to them, and focus on the scaling laws of secret communications without computational assumptions. In contrast, our private communications method is more practical in the sense that it does not need to control the received signals at the eavesdroppers. On the other hand, we stress that our private communications method is to illustrate the application of our OT21 protocol. We choose this application because it is simple and easy to understand, *not* because our private communications method is more efficient than the existing works on private communications.

III.MODEL OF WIRELESS CHANELL

Suppose we have two parties *A* and *B* connected through a wireless channel between them. The magnitude of in phase component should be *h,* which follows a Gaussian distribution. Here *h* can be considered as a stochastic process; to represent the value of *h* at time *t* we use *h*(*t*).One thing is noted that both the parties do not know the precise values of *h*(*t*). Only they have to make an estimates .To initiate the communication process there will be a sharing of probe signal *s*(*t*). Suppose at time t1, *A* receives a probe signal send by *B.* Now party *A* sends a probe signal and party *B* receives it at time *t*2. Both the parties now estimate the channel using their received probe signals.

The received signals of A and B can be shown as follows

$ra(t1) = h(t1)s(t1) + na(t1)$…….. (1)

$rb(t2) = h(t2)s(t2) + nb(t2)$…….. (2)

where $na(t1)$ shows a receiver noise at party A and $nb(t2)$ shows a receiver noise at party B.

METHOD OF QUANTIZATION

When A and B have obtained their estimates ˆha and ˆhb, respectively, they quantize these channel estimates into bit strings using a quantization function Q. The function Q is defined as follows:

Q(x)= 1 if x>q+

Otherwise

Q(x)= 0 if x<q−

where

q+ and q− are derived from the mean and standard deviation of channel estimates. Denote the mean by μ and the standard deviation by σ.

Let α(α>0) be a system parameter. We have $q+,- = \mu \pm \alpha \cdot \sigma$.

REQUIREMENTS FOR OT AND SECURITY MODEL

The goal of this paper is to build OT (Oblivious Transfer) between node *A* and node *B*. In Section III, we describe how to build this protocol, and use this method of quantization. Now to build OT , there are requirements for it. Assume that *A* has two bits *b*0 and *b*1 as her input, and that *B* has a bit *s* as his input. The requirements for an OT.

1) First the node *B* gets the bit *bs*;

2) Now the node *B* do not have any information about

*b*1−*s*;

3) Similarly node *A do* not have any information about *s*.

This model shows that each node follows the protocol, but they may be curious in learning private information that they are not supposed to learn. Furthermore, eavesdropping by outsiders (i.e., parties not supposed to participate in the protocol) are allowed in our model.

IV. OT BASED ON WIRELESS CHANNEL CHARACTERISTICS

Using the probing, estimation, and quantization process

described , now we design an OT21 protocol and analyze it. *The* OT protocol consists of two stages. The first stage, where the two parties send multiple probe signals to each other. Estimate the channel, and now convert the estimates into bits, using the quantization method described in Section II. (Recall that the time interval between each pair of probe signals is within the coherence time, but the time interval between any two different pairs of probe signals is more than the coherence time.) The two parties terminate the first stage as soon as each of them has obtained at least *N* bits, where *N* is an even number.

V. APPLICATION : PRIVATE COMMUNICATIONS

This application deals with the private communication between two communicating parties by using a common secret key *k* between them. This is similar to the symmetric key encryption and also used in decryption method of cryptography. The requirements for this communication are initially *A* send confidential message and *B* reply for the same, the condition is that the key should be same. If the key is different then there will be no reply from *B* when *A* send a confidential message.

The message send by *A* does not known to any eavesdropper. This method of private communication is very much similar to the symmetric key encryption and also to the symmetric key decryption used in cryptography. But this method is not identical to symmetric key encryption and the decryption. This model is different than the cryptography model we generally used, since here in this model of private communication we are not using ciphertext in traditional sense.

VI. APPLICATION : PRIVACY PRESERVING PASSWORD VERIFICATION

To identify the user password verification is one of the method which is popular today. In wireless LANs, Many base stations at the beginning of sessions authenticate users using their passwords. But the risk of hacking of password is more when users send passwords by using wireless links. So it is necessary to provide privacy protection of password ,as password is going to use for authentication. In this method one wireless device has to identify the password from other device and with privacy preserving of the password. Following are the major requirements for this method. Initially wireless device *A has to send a password* entity that matches by the *B*'s record and suppose it should be matches by it then only accepted. Another possibility is that if it is not matches by the record of *B then* it will be rejected by *B.* The thing should note here is only *A* has to match a password with

B's record and nothing more than it. The same thing is happened opposite in case for the *B* also which learn nothing about the password rather it matches or not only. It is an advantage of this application is that the password matching process and off course the password does not known to the eavesdroppers that can attack on this process which is not possible due to privacy preserving password verification technique.

VII. CONCLUSION

Here , we present an OT protocol with two applications. This protocol does not depend on computational assumption and it is a major advantage of this protocol. It is found that in previously the major cryptographic tools also broken by the attackers and hence the need for such a technique which can able to provide strong security in wireless area is the requirement which can fulfill through this approach. Our work considered to be a step towards building wireless security which do not depends on computational assumptions although if we consider the speed in term of performance then this protocol is still not that much fast as the generally used OT based on computational assumptions.

REFERENCES

FIPS Publication 197, *Advanced Encryption Standard*. NIST, 2001. X. Wang and H. Yu, "How to Break MD5 and Other Hash Functions," in *EUROCRYPT 2005*. Springer Berlin / Heidelberg, 2005, pp. 19–35.

X. Wang, H. Yu, and Y. L. Yin, "Efficient Collision Search Attacks on SHA-0," in *CRYPTO 2005*. Springer, 2005, pp. 1–16.

Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *WiSe '06*. ACM, 2006, pp. 33–42

C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *ISIT'06, IEEE*, July 2006, pp. 2593– 2597.

B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, key generation from signal envelopes in wireless networks," in *ACM* IEEE, pp 1541-1544.
A. Sayeed and A. Perrig, "Secure wireless communications: keys through multipath," in *ICASSP 2008*, 2008, pp. 3013–3016.

S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy: extracting a secret key from an unauthenticated wireless channel," in *MobiCom '08*. ACM, 2008, pp. 128–139..

S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE. Trans. Mob. Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010

J. Kilian, "Founding crytpography on oblivious transfer," in *STOC '88*. New York, NY, USA: ACM, 1988, pp. 20–31.

C. Cr´epeau and J. Kilian, "Achieving oblivious transfer using weakened security assumptions," in *FOCS'88*, Oct 1988, pp. 42–52.

C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensic Secur.*, vol. 5, no. 2, pp. 240 –254, 2010.

J. Tugnait, L. Tong, and Z. Ding, "Single-user channel estimation J. Tugnait, L. Tong, and Z. Ding, "Single-user channel estimation.

T. Rappaport, Wireless Communications: Principles and Practice.Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

O. Goldreich, *Foundations of Cryptography*. Cambridge U. Press Y. Liang, H. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470–S. Ross, *A First Course in Probability*. Upper Saddle River, NJ, USA: Prentice Hall, 2002.

W. Hoeffding, "Probability inequalities for sums of bounded random variables," *J. Am. Stat. Assoc.*, vol. 58, no. 301, pp. 13–30, 1963..

Y.-F. Chang, "Non-interactive t-out-of-n oblivious transfer based on the rsa cryptosystem," *Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on*, pp. 45–50, 2007.