ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (22-28), Month: April - June 2014, Available at: www.researchpublish.com

A Robust Air key Management using buffer concept

[1]B.BINDHU, [2]MRS.C.FELSY

[1]PG Student, Department Of Computer Science, Ponjesly College of Engineering, Nagercoil, Tamilnadu, India
[2]Asst. Prof, Department Of Computer Science, Ponjesly College of Engineering, Nagercoil, Tamilnadu, India

Abstract: **Key management between nodes can be addressed when public key infrastructure (PKI) or an online trusted third party (TTP) is available. These solutions cannot always be applied to resource constrained devices operating in pervasive environments because of both the lack of either a PKI or a TTP, and bandwidth overhead required by asymmetric cryptography. Robust air key management to allow two wireless communicating parties to commit over-the-air on a shared secret, even in the presence of a globally eavesdropping adversary. The Existing system no crypto but just plain text message exchange, for each one bit transmission, the sender of that bit not its value, which is indeed exchange in clear text. The proposed system using alpha algorithm in which a buffer is used to store all the data to be transferred from node to node in the network so that the transfer of data will be efficient. While sending the data bit by bit if any bit losses then particular bit will be stored in the buffer.**

***Keywords*: key management, over the air (OTA), trusted third party (TTP).**

I. INTRODUCTION

Network Security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Secure key establishment between parties can be addressed when public key infrastructure or an online trusted third party is available. If not another operation could to be use the Diffie-Hellman solution [1]. Private conversation between two people with no prior acquaint also discusses how the theories of communication and competence is a common occurrence in business, however, and it situation are beginning to provide the tools to solve cryptographic unrealistic to expect initial business contacts to be postponed problems of long standing is long enough for keys to be transmitted by some physical means. Each user of the network can therefore news supply the equivalent of a written signature. This enables same time, theoretical developments in information theory and any user of the system to send a message to any other user computer science show promise of providing provably secure enciphered in such a way that only the intended receiver is cryptosystems, changing this ancient art into a science A third preventing the unauthorized extraction of information from communications over an insecure channel order to use crypto to grapy are examined. Widening applications of teleprocess- raphy to insure privacy, however, it currently necessary for thing have given rise to a need for new types of cryptographic communicating parties to share a key which is known to no systems, which minimize the need for secure key distribution one else. This is done by sending the key in advance over some channels and supplies the equivalent of a written signature. This secure channel such a private courier or registered mail

A preliminary solution addressing the Key establishment issues was provided in [2]. Shave is based on initial key exchange followed by exchange and comparison of sensor data for verification of key authenticity. Shack, in contrast, is based on matching features extracted from the sensor data to construct a cryptographic key. The classification algorithms used in our approach are shown to robustly separate simultaneous shaking of two devices from other concurrent movement of a pair of devices, with a false negative rate of under 12 percent. A user study confirms that the method is intuitive and easy to use, as users can shake devices in an arbitrary pattern. For mobile users, it is of potentially great value to associate a personal device with another mobile device in a spontaneous manner, without need for the involved devices to have prior knowledge of each other. Spontaneous associations can be for the purpose of short-lived interactions.

Establishing a new secret without preconfigured information and avoiding asymmetric cryptography is a challenging topic that has been previously undertaken in mainly two ways: leveraging anonymous channel [3] the effectiveness of secret key extraction, for private communication between two wireless devices, from the received signal strength (RSS) variations on the wireless channel between the two devices. We use real world measurements of RSS in a variety of environments and settings Building on the strengths of existing secret key extraction approaches, we develop an environment adaptive secret key generation scheme that uses an adaptive loss quantizes in conjunction with Cascade-based information reconciliation and privacy amplification.

Public key cryptography consumes significant amount of computing resources and power which might not be available in certain scenarios (e.g., sensor networks). More importantly, concerns about the security of public keys in the future have spawned research on methods that do not use public keys[4]Quantum cryptography is a good example of an innovation that does not use public keys. It uses the laws of Quantum theory, specifically Heisenberg's uncertainty principle, for sharing a secret between two end points. Although quantum cryptography applications have started to appear recently.

*Contribution :*This paper presents, robust air key management protocol that guarantees secret key establishment in presence of a global eavesdropper without relying on cryptographic primitives. Show how the transmission power of cooperating parties can be tuned in order to mitigate the adversarial capabilities. Our theoretical results showing the security, effectiveness, and efficiency of as a crypto-less key establishment algorithm are supported by extensive simulations.

Organization: Next section surveys related literature while section III introduces the adversarial model and a brief overview of our solution. Section IV presents the details of our crypto-less on the air key establishment protocol and section V shows its security analysis. Simulation results and discussion follows in section VI and VII, respectively, section VIII introduces practical consideration on the usage of our protocol. Finally, some concluding remarks are reported in section IX.

II. RELATED WORK

Secret key establishment between resource constrained devices realized without use of crypto function has been undertaken in mainly two different ways: extracting secret bits by observing the same physical phenomenon or exchanging secret bits anonymously without using crypto functions.

Physical-layer identification of wireless devices, commonly referred to as Radio Frequency (RF) fingerprinting, is the process of identifying a device based on transmission imperfections exhibited by its radio transceiver. It can be used to improve access control in wireless networks, prevent device cloning and complement message authentication protocols. This paper studies the feasibility of performing impersonation attacks on the modulation-based and transient-based fingerprinting techniques [5] [6]. Both techniques are vulnerable to impersonation attacks; however, transient-based techniques are more difficult to reproduce due to the effects of the wireless channel and antenna in their recording process. We assess the feasibility of performing impersonation attacks by extensive measurements as well as simulations using collected data from wireless devices. We discuss the implications of our findings and how they affect current device identification techniques and related applications.

Cryptographic techniques are essential for the security of communication in modern society [7]. As more and more business processes are performed via the Internet, the need for efficient cryptographic solutions will further increase in the future. Today, nearly all cryptographic schemes used in practice are based on the two problems of factoring large integers and solving discrete logarithms. However, schemes based on these problems will become insecure when large enough quantum computers are built. The reason for this is Shor's algorithm, which solves number theoretic problems such as integer factorization and discrete logarithms in polynomial time on a quantum computer. Therefore one needs alternatives to those classical public key schemes. Besides lattice, code and hash based cryptosystems; multivariate cryptography seems to be a candidate for this. Additional to their (believed) resistance against quantum computer attacks[8], multivariate schemes are very fast and require only modest computational resources, which makes them attractive for the use on low cost devices such as RFID chips and smart cards. However, there remain some open problems to be solved, such as the unclear parameter choice of multivariate schemes, the large key sizes and the lack of more advanced multivariate schemes like signatures with special properties and key exchange protocols. In this dissertation we address two of these open questions in the area of multivariate cryptography. In the first part we consider the question of the parameter choice of multivariate schemes. We start with the security model of Lenstra and Verheul, which, on the basis of certain assumptions like the development of the computing environment and the budget of an attacker, proposes security levels for now and the near future. Based on this model we study the known attacks against multivariate schemes in general and the Rainbow signature scheme in particular and use this analysis to propose secure parameter sets for these schemes.

First, we use an 802.11 development platform with customized logic that extracts raw channel impulse response data from the preamble of a format-compliant 802.11a packet. We show that it is possible to practically achieve key establishment rates of ~ 1 bit/sec in a real, indoor wireless environment. To illustrate the generality of our method, we show that our approach is equally applicable to per-packet coarse signal strength measurements using off-the-shelf 802.11 hardware. In this paper we explore an alternative for building cryptographic services by exploiting an untapped resource-the wireless channel itself. The specificity of the radio channel between two wireless devices and its rapid decor relation with distance, provide a basis for the creation of shared secret information, such as cryptographic keys, even in the presence of an eavesdropper.

III. SYSTEM MODEL

Our scenario is constituted by a couple of fixed radio-equipped device ,hereafter A and B and an adversary here after Advent assumptions are made on the communication protocols,i.e.,IEEE 802.11,IEEE 802.15.4,GSM,Bluetooth.

A. Adversarial Model

As for the adversarial radio eavesdropping capabilities, she can perform global or local eavesdropping. The fundamental to know the relative distance against A and B.

$$\mathbf{d}=\surd\boldsymbol{G}\frac{\boldsymbol{T}}{\boldsymbol{R}}$$

G takes into account the characteristics of the transmitter and receiver antennas R is the received power. Equation represents the signal path loss, i.e difference between the actual transmitted and received power, in free space environment. However, we take a conservative taking into account noise effect due to multipath fading. Noise do help establishment effect of a secret key bit under a powerful adversary model; that is, global eavesdropper. The solution leverages no crypto but just plaintext messages exchange. Indeed, the security of the solution relies on the difficulty for the adversary to correctly identify, for each one-bit transmission, the sender of that bit not its value, which is indeed exchanged in clear text. Requires exchanging a few one-bit messages between the parties for the shared secret to be built and requires only one hash computation for each generated secret key. Computing capabilities are not constraints to energy consumption. Communication channels are prone to packet loss.

B. On channel Anonymity

The security of solution strictly depends on the factor: the channel Anonymity. In fact, for each correct guess of the message source ADV discloses one secret key bit. There are two main attacks that can be performed against channel anonymity: Position guessing, by measuring the received signal strength, and radio source identification by means of physical layer analysis. Both the previous attacks aim at discriminating the peers involved in the key establishment protocol i.e., given an eavesdropped message, the challenge is constituted by guessing the actual source.

IV. SECRET KEY ESTABLISHMENT

In this work we assume all the communication packets are anonymized,i.e.,the source and the destination addresses does not reveal the real sender. For instance, a sender could randomly decide whether to use own ID or the receiver ID to fill in the sender field.

```
Algorithm 1:
Secret key establishment between A and B:
        Secret bits transmission - A side.
Let H (·) be a cryptographic hashfunction.
Let KA
 $ → [0,1] K.
Let T be the current transmission power.
Let pm be the minimum transmission power
Let pm, . . . , PM be the power transmission levels
A (B) randomly chooses the transmission power
T <−[pm, ...PM];
for i <-1 to K do
/*Select a random waiting time within the
Slot: Elapsed is true when such time is elapsed, False
*/ while not Received AND not Elapsed do
Skip
        End
        if not Received then
/* Extract the ith bit */
         KA[i]; /* if B: b   KB[i]; */
        Ks[i] = b;
        Send < ¬b >; /* if B: Send < b >;
*/end
 /* Wait for the current slot to expire.
*/ Elapsed = FALSE; Received = FALSE;
        End
/* Shared secret key generation
*/ Ks = H (Ks);
```

```
Algorithm 2:
         Secret key establishment between A and B:
         Secret bits reception - A side.
         let Ks be the shared secret key.
         /* A (B) receives the secret bit b
        */ Receive < b >;
        Received = TRUE;
        Ks[i] = b; /* if B: Ks[i] = ¬b;
```

Dealing with packet loss:

Wireless communication channel are prone to packet loss, and this may prevent secret establishment. In particular, if one packet get lost due to a wireless channel impairment, A and B lose their synchronization, ant this will prevents the generation of the shared secret **K**

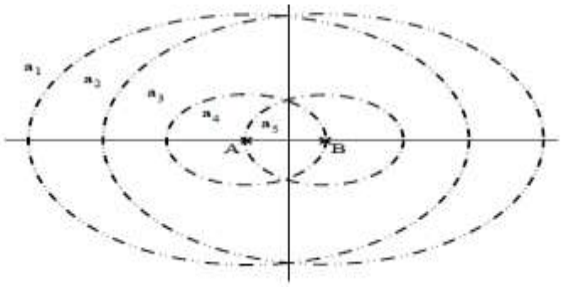


Fig 1.Minimum and Maximum Transmission powers

V. ANALYSIS

Fig. 1 shows A and B Positions with their radio coverages, i.e., a single dot dashed line is associated to the minimum transmission power. While double dot dashed line is associated to the maximum Transmission power.

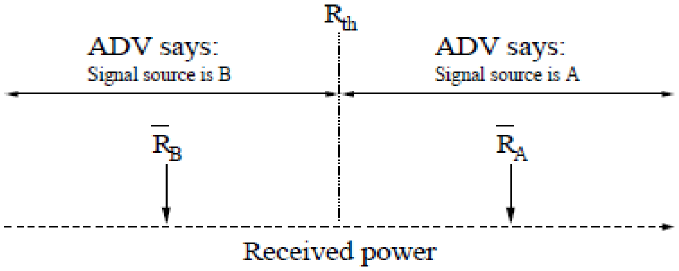


Fig.2 Signal source guessing depends on the current received power

VI. RESULTS

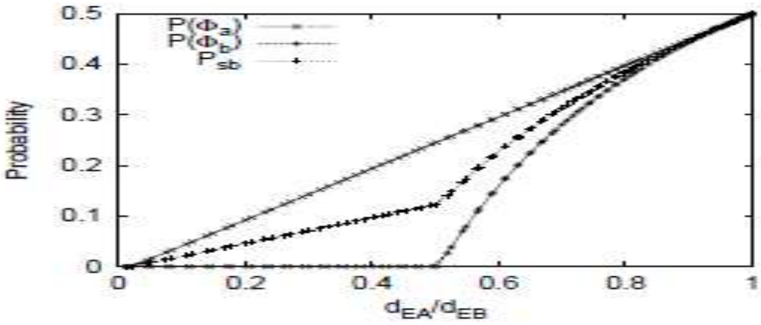


Fig. 3: Theoretical trends associated to the secret-bit transmission

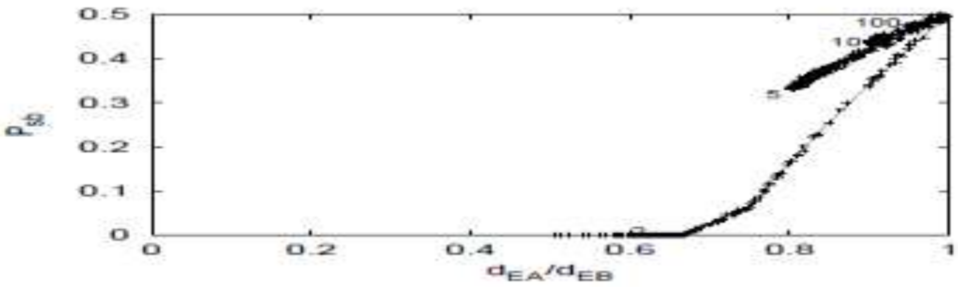


Fig. 4: Secret bit transmission probability contains (2,5,10,200)

VII. DISCUSSION

The maximum power P_m can be leveraged to increase the probability of secret bit transmission: Even if ADV gets closer to one of the peers, increasing PM can hide the actual signal source. In particular, when ADV belongs to position maximum transmission power.

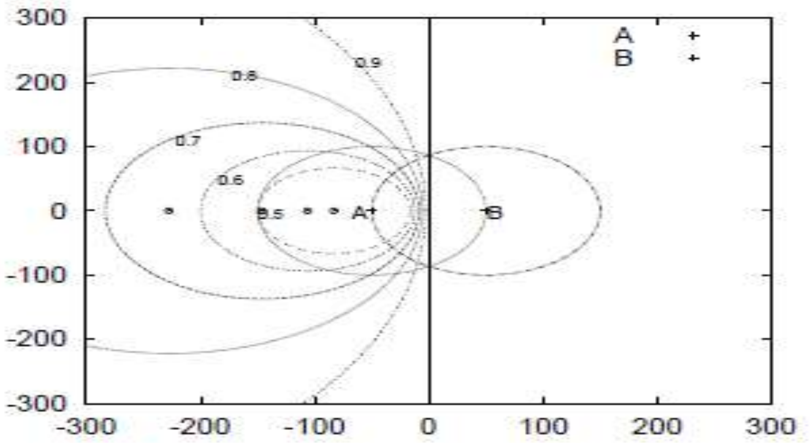


Fig. 5 Number of transmission to commit on secret bit key length, respectively as function

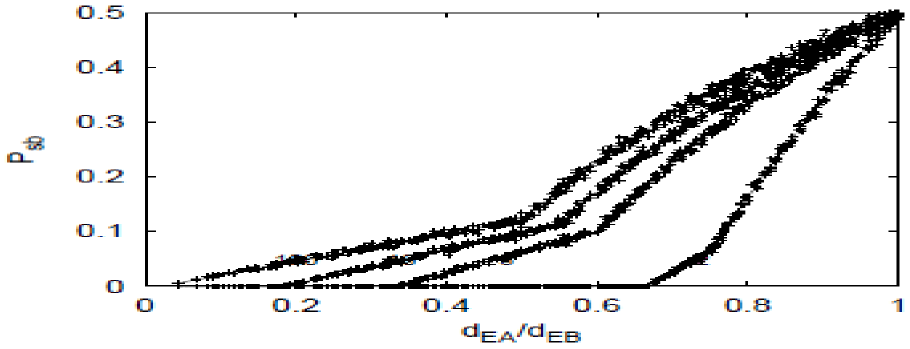
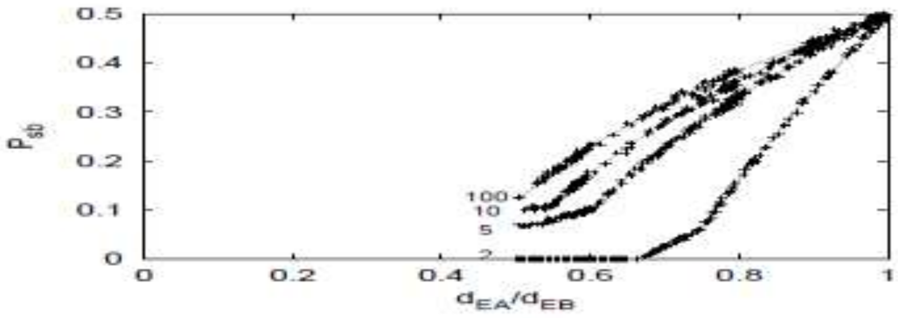


Fig. 6 Secret-bit transmission probability

A. *Adversarial positions*

Qualitative analysis about the relation between the adversarial positions to provide an estimation minimum number of transmission needed to commit on a shared key show the two peers A and B deployed on a grid with the circles corresponding to their minimum transmission power, 64 secret key length needs about 160 transmission for the given transmission power.



IX. CONCLUSION

In this work we have introduced robust air key management t that allows two peers to commit on a shared secret key without using reconstituted secrets or symmetric crypto function requires to exchange a few one bit messages between the parties for the shared secret to built requires only one hash computation for each generated secret key. given efficiency ,it is particularly suited for resources constrained wireless devices, as well as for those scenarios where energy saving is at premium, such as smart phones. A thorough analysis of the security of the proposed protocol is provided. Further extensive simulation confirm our finding

References

[1] Azimi-Sadjadi.B,Kiayias.A(2007)'Robust key Generation from signal envelopes in wireless networks'in proc.CCS'07.

[2] Diffie.W, Hellman M. E(1976) 'New directions in cryptography' IEEE Trans. Inf. Theory.

[3]Ganeriwal.S,popper.C,Capkun.S,Ding,W.and Brown, L. D., Hua, H., and Gao, C.MarchioniniSrivastava,M.B(2008)'Secure time Synchronization in sensor network' ACM Trans. Inf

[4] Gerders.R, Mina.M (2012)'Physical Layer identification of wired Ethernet devices' IEEE Trans. inf. Forensics Security.

[5] Jana.S, Premnath.S.N, Clark.M, Kasera.S.K, Patwari.N, Krishnamurthy S.V (2009) 'On the effectiveness of secret key extraction for wireless signal strength in real environments' inProc. MOBICOM.

[6] Jan.J, Goh,W.L, Kong.Z.H (2010)' Random Number generator for low power cryptographic application'in proc. 2010 Int. Soc Design Conf. (ISOCC).

[7]Lenstra.A,,verheul.E.R(1999)'SelectingCrytogphicKeys'.

[8]Mathur.S, Ye.N.M.C, Reznik.A (2008)' Radio-telepathy:Extracting a secret Key from an unauthenticated wireless channel', in proc. mobiCom.

[9] Mayrhofer.R, Gellersen.H (2009) 'Shake well before use: Intuitive and secure pairing of mobile devices' IEEE Trans. Mobile Computer.

[10]VerbiskiyE,A, Tuyls.p, obic.C, Schoenmakers.B, Skoric.B (2010) 'Key extraction from general nondiscrete signals' IEEE Trans. Inf. Forensics Security.

Authors Bibliography

B.Bindhu she received her Bachelor degree in Computer Science and Engineering fromPonjesly College of Engineering, Nagercoil, Affiliated to Anna University, Chennai in 2012.Now she is doing her II 2nd yr Post Graduate degree in Ponjesly College of Engineering, Nagercoil Affiliated to AnnaUniversity, Chennai, Tamilnadu.