International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 7 Issue 1 –MARCH 2014.

A SECURE KEYLESS CYPTOSYSTEM

Mr.T.P.Jayakumar M.E.,(Ph.D.,)+,R.Saranya M.E(CSE)*

***-Department of Computer Science and Engineering, Maharaja College of Engineering and Technology, Perundurai**

+-Head of the Department, Department of Computer Science and Engineering, Maharaja College of Engineering and Technology, Perundurai

ABSTRACT

Key Establishment between two nodes is done by collecting the accelerometers data by shaking of the devices coupled together: shared secret collected from the accelerometers data that proved to be correlated. By establishing a shared secret without preconfigured information and then avoiding asymmetric cryptography is a new challenging topic that has been undertaken mainly of two ways: leveraging anonymous channels or adopting Received Signal Strength key establishment protocols. This technique is done based on the extraction of shared secrets from the collection of the RSS values at both the peers. Thus the two nodes can be shared their values though there is an easy of sharing the secrets by using the Time Based Protocol. COKE (Crypto-less Over-The-Air Key Establishment) is based on sharing of content by hiding only the source-idand sending the content in bit by bit within a fraction of seconds.

Key establishment can be addressed by a protocol named TIME BASED PUZZLE. This protocol enables the nodes to share information based on the puzzle.A new Crypto-less key is established for wireless communicating parties to commit on a shared secret key. This explains no crypto but just plaintext message exchange. Hiding the source address and the data, where data is hided using the puzzle. Both the data and the puzzle are sent one by one within a fraction of seconds. Puzzle is like a Password to carry that information. There is a buffer on the receiver side to store the data in which it is received. The receiver has to solve the puzzle to extract the information.

INDEX TERMS: Anonymous channels, RSS, Accelerometers, Time Based Puzzle, COKE

I INTRODUCTION

SECURE KEY establishment can be addressedbetween two parties when Public Key Infrastructure (PKI) or an Online Trusted Third Party (TTP) is available. If not, another way is to use the Diffie-Hellman solution. These solutions unfortunately, cannot always be applied to resourceconstraineddevices operating in pervasive environments becauseof the lack of either a PKI or a TTP, the highcomputation and bandwidth overhead required by asymmetriccryptography.A preliminary solution was the addressingof the key establishment issue was provided. A kineticprocedure included here is that collecting accelerometers data during the shakingof the two devices when coupled together. The preconfigured information and avoiding asymmetric cryptography is one of the challenging topic that has been already undertaken inmainly of two ways: they are the leveraging anonymous data that are proved to be correlated. Though such an approach is mostly effective,shared secret data comes from the accelerometers for these devices that can has been shaken together. Establishing a new shared secret without the usage of channelsor adopting Received Signal Strength (RSS-based) keyestablishment protocols. This technique is based onextracting those secrets from the collection of the RSSvalues received at both the peers. There are also some issues still that have to be resolved by using the techniques such as asymmetric effects introduced by the multipath fadingand also the need for a very dynamic

*Contribution:*This paper presents a novel probabilistic protocol that guarantee a secret transmission of data by hiding the content of the packet using the puzzle. The puzzle is like a password to carry that information. Both address and the data are sent one by one to the sender with in a fraction of seconds. The Puzzle is like the matching of the pictures and the data will be stored on the receiver side buffer until the receiverextract the packet by solving the puzzle.

environment to generate key establishmentwith sufficient entropy.Crypto-less key establishment protocols is mainly based on anonymous channels that have been introduced for the first time bysubsequent improvement. The main idea that relies on establishing a shared secret key between two peers without using the cryptography function is the leveraging source of indistinguishability of anonymous channels. Anonymous channels guarantee that an adversary cannot able to easily identify that actual signal source even if it is able to eavesdrop all the transmitted messages. During such scenario, two peers can exchange all the bits of a secret message but there is no possible for an adversary to combine the current transmitted bit to the actual source. Thus crypto-less algorithms are mainly useful in *pairing* of resource-constrained devices due to the fact that they are not rely on battery expensive calculations. The security of these approaches are strongly relies on the temporal and spatial indistinguishability.

The information is extracted in a secure way even when an adversary is tried to attack the data. There is no need for cryptographic functions so the encryption and decryption time is reduced rather thansolving the Puzzle using the Time Based Puzzle Protocol.

that is the proposed algorithm involve to put together two peers and shake them collect the accelerometer readingsand then the new connection is established between the two.Secret key establishment between the several resource constrained devices is realized that without usingthe cryptographyfunctions, the sharingsecret has been undertaken in mainly of two different ways: Extracting those secret bits between peers by observing the physical

II RELATED WORK

There is some physical phenomenon which is used to extract the shared secrets between two peers. Multipath fading introduce the problem of asymmetries on the received power but theyalso proposed few algorithms to recover these errors and also eventually they alsoagreed on a shared secret key. The accelerometer is used to verify that whether the two peers going to share the data are carried by the same user and also to extract shared secrets by observing those accelerometers readings, Another the sender and the receiver can know the actual value of that transmitted bit. Thus this approach relies on the anonymity of both the sender as well as the receiver obtained by The accelerometer collect the sender and receiver identity by shaking those devices and make them together that is the signal source cannot be identified by the attacker because they are only randomized by the accelerometers shaken procedure. In Crypto-less protocols security mainly relies on two factor: Temporal and Spatial indistinguishability. Where the former can be easily achieved, the latter ismore difficult due to the *power analysis*.While the “shaking” as an effective solution to an analysis attack, random transmission power can definitely phenomenon or by exchanging those bits anonymously without using these crypto functions. By using accelerometers collect the values between the two peers and make them to share the data. Thus the two peers can share their data by establishing the key between them. approach is the key exchange using keyless cryptography that is the proposal to create and distribute a secret key by hiding only the identity of the transmitterand not the whole packet that is without hiding the content. Thus the adversary cannot able to know the value of the secret data bit and also the sender of that single bit. There is also another algorithm which is pairing of two peers that is based on exchanging packets with the source field and it is chosen as a function of the secret bit. Thus by sharingthe data by this way only possible to share the data easily. The puzzle generator generates the puzzle and the time slot is included in each and every packet, so that receiver can extract the data easily using the TIME BASED PUZZLE ALGORITHM shared already.

improve crypto-less protocols performance even for static devices.

III PROPOSED METHODOLOGY

In this paper the messages shared in secured manner by means of TIME BASED PUZZLE PROTOCOL. The packet with the sender’s identity as well as the content is hided,the content is hide by using puzzle. Solving the puzzle is like mapping the images. The puzzle is like a password so that the attacker cannot able to extract the content by knowing the information which was collected by them using accelerometers

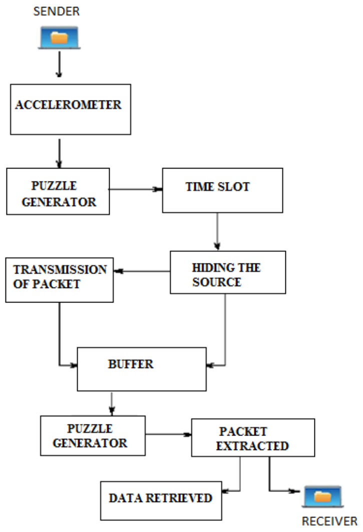

Fig.1.Architecture Diagram

The sender’s identity is also hided so that an attacker cannot able to identify the source easily. If the receiver is failed to solve the puzzle within the time slot they has to extract the packet which is stored on the receiver side buffer until they solve the puzzle that is by mapping the images. Thus the data will be more secure than other crypto functions.

IV IMPLEMENTATION MECHANISM

The puzzle is designed to foil attempts of a solver to exploit parallel or distributed computing to speed up the computation. The computation required to solve the puzzle is "intrinsically sequential". The problem is to compute 2^(2^t) (mod n) for specified values of t and n. Here n is the product of two large primes, and t is chosen to set the desired level of difficulty of the puzzle. Note that the puzzle can be solved by performing t successive squaring modulo n, beginning with the value 2. That is, set

W(0) = 2

W(i+1) = (W(i)^2) (mod n) for i>0,

and compute W(t). There is no known way to perform this computation more quickly without knowing the factorization of n.

The value of t was chosen to take into consideration the growth in computational power due to "Moore's Law". Based on the SEMATECH National Technology Roadmap for Semiconductors , the expectation in internal chip speeds to increase by a factor of approximately 13 overall up to 2012, when the clock rates reach about 10GHz. After that improvements seem more difficult, but the estimation is that another factor of five might be achievable by 2034. Thus, the overall rate of computation should go through approximately six doublings by 2034. The puzzle will require 35 years of continuous computation to solve, with the computer being replaced every year by the next fastest model available. Most of the work will really be done in the last few years, however. An interesting aspect is how to protect such a computation from errors. If you have an error in year 3 that goes undetected, you may waste the next 32 years of computing. The authors proposed a slick means of checking your computation as you go, as follows. Pick a small (50-bit) prime c, and perform the computation modulo cn rather than just modulo n. You can check the result modulo c whenever you like; this should be a extremely effective check on the computation modulo n as well.

In order to allow the LCS director in the year 2034 (or whenever) to verify a submitted solution, we have arranged things so that solving the puzzle also enables the solver to factor the modulus n, as described below.

Of course, one way to break the puzzle is to factor the modulus n directly. But we have chosen a 2048-bit modulus, which is unlikely to be factored in the given time frame without a breakthrough in the art of factoring. Just as a failure of Moore's Law could make the puzzleharder than intended, a breakthrough in the art of factoring would make the puzzle easier than intended. Here is a smaller example of the puzzle.

Suppose n = 11*23 = 253, and t = 10. Then we can compute:

2^(2^1) = 2^2 = 4 (mod 253)
2^(2^2) = 4^2 = 16 (mod 253)
2^(2^3) = 16^2 = 3 (mod 253)
2^(2^4) = 3^2 = 9 (mod 253)
2^(2^5) = 9^2 = 81 (mod 253)
2^(2^6) = 81^2 = 236 (mod 253)
2^(2^7) = 236^2 = 36 (mod 253)
2^(2^8) = 36^2 = 31 (mod 253)
2^(2^9) = 31^2 = 202 (mod 253)
w = 2^(2^t) = 2^(2^10) = 202^2 = 71 (mod 253)

Thus, the "w" value computed for the puzzle is 71 (decimal), which is 47 (hex). If we have a "z" value for the puzzle of 13 (hex), then the "secret message" for the example is (47 XOR 13) = 54 (hex). (The secret message should then be interpreted in ASCII at 8 bits per character).

Thus to solve the puzzle computations are needed. Mapping the images is more important to extract the content. The attacker cannot able to know these computations to extract the data or else he does not know the mapping of images by using this algorithm. This method is more useful than any other crypto function to share the data without using the cryptography.

V CONCLUSION

In this work we have introduced A SECURE KEYLESS CRPTOSYSTEM, rather than a crypto-less over-the-air key establishment algorithm that allows two peers to commit on a shared secret key without using secrets or asymmetric crypto-functions. We evaluated the effectiveness of secret key extraction from the received signal strength (RSS) observations in wireless channels using extensive real world measurements. Hiding the packet that is source-id and the content is hide by using puzzle.

Solving the puzzle is by mapping the images. The attacker cannot able to identify easily the source-id to extract the content. By given its efficiency, it is particularly suited for resource constrained wireless devices, as well as for those wireless scenarios whereenergy saving is atpremium, like smartphones.

VI REFERENCES

[1] B. Danev, S. Capkun, R. J. Masti, and T. S. Benjamin, “Towards practical
identification of hfrfid devices,” *ACM Trans. Inf. Syst. Security*,
vol. 15, no. 2, pp. 7:1–7:24, Jul. 2012.

[2] R. Gerdes, M. Mina, S. Russell, and T. Daniels, “Physical-layer identification
of wired ethernet devices,” *IEEE Trans. Inf. Forensics Security*,
vol. 7, no. 4, pp. 1339–1353, Aug. 2012.

[3] P. Barsocchi, G. Oligeri, and C. Soriente, “Shake: Single hash key establishment
for resource constrained devices,” *Ad Hoc Networks*, vol.
11, no. 1, pp. 288–297, Jan. 2012.

[4] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, “Attacks onphysical-layer identification,” in *Proc. WiSec’10*, 2010, pp. 89–98,ACM.

[5] E. A. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, and B. Škorić,“Key extraction from general nondiscrete signals,” *IEEE Trans. Inf.Forensics Security*, vol. 5, no. 2, pp. 269–279, Jun. 2010

[6] E. Matthew and Y. Blent, Active Attacks Against Modulation-BasedRadiometric Identification Rensselaer Polytechnic Institute, Departmentof Computer Science, Tech. Rep., 2009.

[7] P. Peris-Lopez, J. C. Hernandez-Castro, J. M. Tapiador, and A. Ribagorda,“Advances in Ultralightweight Cryptography for Low-CostRFID Tags: Gossamer Protocol,” in *Information Security Applications*.Berlin, Heidelberg: Springer-Verlag, 2009, pp. 56–68.

[8] G. de Meulenaer, F. Gosset, F.-X.Standaert, and O. Pereira, *On theEnergy Cost of Communication and Cryptography in Wireless SensorNetworks*, ser. WIMOB’08. Los Alamitos, CA: IEEE Computer Society,2008, pp. 580–585.

[9] R. Mayrhofer and H. Gellersen, “Shake well before use: Intuitive andsecure pairing of mobile devices,” *IEEE Trans. Mobile Comput.*, vol.8, no. 6, pp. 792–806, Jun. 2009.

[10] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S.V. Krishnamurthy, “On the effectiveness of secret key extraction fromwireless signal strength in real environments,” in *Proc. MOBICOM2009*, 2009, pp. 321–332.

[11] M.Wilhelm, I. Martinovic, and J. B. Schmitt, “Secret keys from entangledsensor motes: Implementation and analysis,” in *Proc. WiSec’10*,2010, pp. 139–144, ACM.

[12] J. Croft, N. Patwari, and S. K. Kasera, “Robust uncorrelated bit extractionmethodologies for wireless sensors,” in *Proc. IPSN’10*, 2010, pp. ACM.

[13] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, “Robustkey generation from signal envelopes in wireless networks,” in *Proc.CCS’07*, 2007, pp. 401–410, ACM.

DI PIETRO AND OLIGERI: COKE CRYPTO-LESS OVER-THE-AIR KEY ESTABLISHMENT 173

[14] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors:How to generate strong keys from biometrics and other noisy data,”*SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, Mar. 2008.

[15] J. Guajardo, B. Škorić, P. Tuyls, S. S. Kumar, T. Bel, A. H. Blom, andG.-J.Schrijen, “Anti-counterfeiting, key distribution, and key storagein an ambient world via physical unclonable functions,” *Inf. Syst. Frontiers*,vol. 11, no. 1, pp. 19–41, Mar. 2009.

[16] P. Barsocchi, G. Oligeri, and F. Potorti, “Measurement-based frameerror model for simulating outdoor wi-fi networks,” *IEEE Trans. WirelessCommun.*, vol. 8, no. 3, pp. 1154–1158, Mar. 2009.

[17] B. Bandemer, C. Oestges, N. Czink, and A. Paulraj, "Physically motivatedfast-fading model for indoor peer-to-peer channels," *Electron.Lett.*, vol. 45, no. 10, pp. 515–517, May 2009.

[18] S. Ganeriwal, C. Pöpper, S. Capkun, and M. B. Srivastava, "Securetime synchronization in sensor networks," *ACM Trans. Inf. Syst. Security*,vol. 11, pp. 23–35, July 2008.

[19] D. Singelee, S. Seys, L. Batina, and I. Verbauwhede, "The communicationand computation cost of wireless security: Extended abstract,"in *Proc. WiSec'11*, 2011, pp. 1–4, ACM.

[20] C. Joumaa, A. Caminada, and S. Lamrous, "Mobility simulation for theevaluation of umts power control algorithms," in *Proc. New Technologies,Mobility and Security, 2008 (NTMS'08)*, Nov. 2008, pp. 1–5.

[21] J. Lan, W. L. Goh, Z. H. Kong, and K. S. Yeo, "A random numbergenerator for low power cryptographic application," in *Proc. 2010 Int.SoC Design Conf. (ISOCC)*, Nov. 2010, pp. 328–331.

[22] C. Lederer, R. Mader, M. Koschuch, J. Grosschädl, A. Szekely, andS. Tillich, *Energy-Efficient Implementation of ECDH Key Exchangefor Wireless Sensor Networks*, ser. WISTP'09. Berlin, Heidelberg:Springer-Verlag, 2009, pp. 112–127.

[23] S.Mathur, N. M. C. Ye, and A. Reznik, "Radio-telepathy: Extractinga secret key from an unauthenticated wireless channel," in *Proc. MobiCom*,2008, pp. 128–139.