European Journal of Computer Science and Information Technology
Vol.2, No.2, pp.9-16, June 2014
Published by European Centre for Research Training and Development UK (www.ea-journals.org)

ROLE OF CRYPTOGRAPHY IN WIRELESSES SENSOR: FUTURE POTENTIAL

Masrat Yousuf Pandith

I.T Skills Department, King Saud University
Riyadh, Saudi Arabia

ABSTRACT: *Wireless Sensor Network (WSN) assists to communicate with limited frequency and bandwidth through the group of independent nodes. WSN has an extensive application in both industrial and commercial areas to manage peril environments incorporating nuclear power plants and wilderness areas. Cryptography is used for writing secret code and it is an ancient technique. Moreover Cryptography is required in data and telecommunications in order to communicate with unreliable medium especially in the internet. Cryptography technique is classified in several ways but for this paper, the technique will be classified on the basis of number of keys used for decryption and encryption. Elliptic Curve Cryptography is an efficient technique in providing security solution for wireless networks. As compared with traditional public key cryptography such as RSA, eclipse curve cryptography attains better result in providing security services. The findings reported that the newly developed protocol was more scalable, less weight and required less memory compared to symmetric based cryptography. This paper concludes that Cryptography is one such technique to confront security problems in WSN. However cryptography alone is not enough to confront WSN problems. It is essential to use the key management process carefully in order to achieve higher security system networks***.***

KEYWORDS*:* Wireless Sensor Network, Cryptography, Elliptic Curve Cryptography, RSA, System networks

INTRODUCTION

WSN (Wireless Sensor Network) is nothing but a collection of independent nodes which help to communicate with limited frequency and bandwidth Akyildiz, Su, Sankarasubramaniam, Cayirci [2002] by monitoring physical as well as environmental circumstances like sound, temperature, pressure, vibration, and motion of various locations [Liu et al., 2002]. WSN is varied from traditional sensor in terms of making intense deployment and coordination for successful execution of their task. For instance, if the precise location of particular event is indefinite, WSN employs single sensory mode to attain closer placement of such task [Bharathidasan et al., 2001]. WSN has wider applications in both industrial and commercial areas to oversee peril environments including nuclear power plants and wilderness areas as it is very tough to examine by means of wired sensors.

Albeit WSN has wider application, it is more susceptible to several threats specifically in the area of military field due to its wireless communication property. At the same time, the validation of sensed data provided by WSNs is vital in many fields. For instance [Caro et al., 2009], in nuclear power plants, the data collected on radioactive levels has transmitted into

base stations should be authentic and have not been tailored at the time of transmission to avoid the errors and possible risks to the works caused by modified data. WSNs are also used in health care system [Caro et al., 2009] to perform similar kind of function as mentioned above. Thus, authentication of data is indispensable for all sectors. However, WSN confront several challenges as compared with traditional networks/computer security because sensors possess limited resources with respect to computing, battery power, memory, and so on [Caro et al., 2009; Lopez & Zhou, 2008]. In order to secure the communication between sensors, security services like key management and authentication are highly important in hostile environment. Sastry and Wagner [2003] identified numerous problems within the user's authentication security given by IEEE 802.15.4 [Yeh et al., 2011] which includes the problems in key management, ACL management and loss of ACL state as a result of power interruptions. Finally the researchers concluded that security provided by IEEE 802.15.4 has several flaws in terms of providing users authentication and solutions for inbuilt problems. One of the important security services to communicate with sensor is cryptographic techniques which can be employed by means of asymmetric and symmetric key functions as well as hash function. As the sensory nodes have constrained resources, a light weighted cryptographic algorithm is required to assist WSN security [Karlof et al., 2004; Perrig et al., 2004].

THE OBJECTIVES OF CRYPTOGRAPHY

Cryptography is an ancient technique which involves in writing secret code. Its history can be traced back from 1900 B.C. Some authors contend that cryptography has appeared instinctively when writing was discovered, with massive applications ranges from diplomatic missives to warfare plans. Soon after, it becomes inevitable in the growth of computer communications. Further, cryptography is used in data and telecommunication while communicating with unreliable medium specifically the Internet. While discussing any application-to-application communication, it is essential to acknowledge certain specific security obligations including:

1. Authentication
2. Privacy/confidentiality
3. Integrity
4. Non-repudiation

Cryptographic technique is not only used to protect data from alteration but also essential for security users authentication. Basically, cryptography is of three types which help to resolve data theft issues: secret key cryptography, public key cryptography, and hash function. In all three types, the first unencrypted data is commonly referred with the name of plain text and two communicating parties involved will be denoted as Alice and Bon. These two names are common in the crypto domain. Further, if the third or fourth party involved and will be denoted as Carol and Dave. The malicious party will be referred as Mallory and eavesdropper will be named as Eve and Trent will be a third party.

CRYPTOGRAPHIC TECHNIQUES

As the WSN fame has increasingly higher in various applications including environmental monitoring, climate change, home automation and traffic monitoring and thus securing WSN secure is always a complicated task. Cryptography technique is classified in several ways but for this paper, the technique will be classified on the basis of number of keys used for decryption and encryption. Below figure 1 clearly depicts the three types of algorithm.

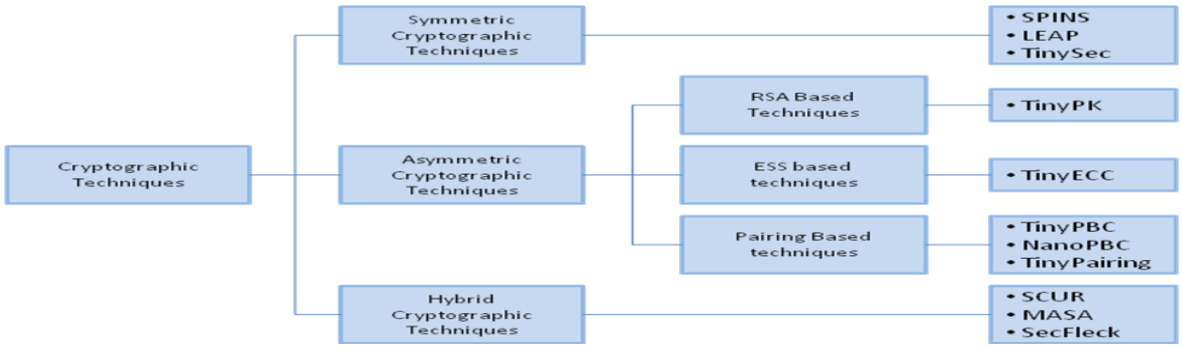

Fig. 1. Cryptographic Techniques.

Secret Key Cryptography (SKC) or symmetric CT: This technique employs only a single key for decryption and encryption.

Public Key Cryptography (PKC) or asymmetric CT: This technique employs two keys: one for encryption and other for decryption.

Hash Functions: Compared with other, this technique employs a mathematical transformation to irreversibly "encrypt" information.

CURRENT WORKS

This section will discuss about the previous studies specifically designed as well as executed to offer security to WSN. Cryptography is one of the important techniques in securing security issues but it is highly questionable whether the cryptography primitives are traditionally used in other network system suitable for security applications. As mentioned before, the low power sensor design is the key problem in cryptography technique and has only less memory and low computation power too. On one side, cryptography must be designed to consume only low memory but at the same time, the design should consider each and every bit transmitted has to consume as much energy/power as implementing hundreds of instructions.

During the past few years, symmetric cryptography has getting importance among researchers because of its energy efficacy. Several solutions regarding security problems have been identified based on the aforementioned technique. For instance, UC Berkeley developed TinySec [Perrig et al., 2002] symmetric encryption and software such as Message Authentication Code (MAC) based on symmetric cryptography for Mica motes. In addition to this, an AES implementation has also encoded on Ember sensor nodes [Beller & Yacobi, 1993; Biryukov & Wagner, 1999; Kohl & Neuman, 1993]. All such aforementioned solutions

followed secret key pre-distribution criteria in the midst of sensors prior to the deployment phase and thereby the adjacent sensors could be later developed by the encrypted communications. The main reason for adopting the criteria is that the less amount of memory prevents nodes from holding massive keys. Despite, several authors contend about the complexities of pre-distribution but it is not that big problem, while think about that the sensor of WSN generally stick with single domain which can be controlled by the similar entity on or before the phase of deployment. At the same time, the design criteria along with the massive communicating nodes lead to the end-to-end unreliable encryption that affects the sensor node scalability. While other researchers contend that the pre-distribution of sensor node is usually common but the physical security of such node is not possible to achieve. From this it is clearly understood that the security of key material is impossible and subsequent compromise of a specific node would provide space for an attacker to generate encrypted data and decrypt the same which can be directed to the sensor node. Thus, the underlying problem in the symmetric cryptography is the shortcomings in the key management technology. However, the alterative of this technique like public-key cryptography was also too costly and impracticable by designers of aforementioned solutions as the computation requirement is varied with the less memory and power/energy that sensor suggest.

In fact, to avoid the use of public-key cryptography and simultaneously to uptake its benefits for authentication purposes and key management, it is vital to run the security protocols of WSN such as SNEP and μTESLA [Haas & M. Perlman, 1998] by means of delayed disclosure of symmetric keys. But by doing this will damages various software and hardware requirement of the nodes. On one hand, it is essential to synchronize the WSN base station and adequate memory so as to store entire symmetric keys but at the same time, the synchronization in the sensor of key management operation is also required. In addition to this, as pointed by [Gaubatz et al., 2004], there is a need to update the keys which are shared among all nodes in regular intervals will aid to develop an expressive protocols as no direct link exists within the sensors.

Though it might perceive that symmetric-key cryptography is suitable for providing WSN with security, it is a common belief in recent days that public-key cryptography is more feasible in terms of providing sufficient security if appropriate protocols are selected [Gaubatz et al., 2005; Wander et al., 2005]. One of the main advantages of this public-key cryptography is that it simplifies key security services and thereby decreases the transmission power as a result of low protocol overhead. But in the past few years, several researchers have rejected this type of cryptographic protocols as it is based on conventional public key security techniques, including verification and creation of signatures, exceed computation capabilities and so on.

In spite of this, many authors [Gura et al., 2004] have shown interest to employ public-key cryptography due to its feasible public-key cryptosystem on 8-bit CPUs. In addition, researchers adapting this technique to sensor node in order to (i) enhance WSNs security, (ii) reduces the difficulties in authentication protocols and key distribution issues, (iii) develop sensors with public key material to circumvent that a captured node compromises the security of the WSN, and so on. With regards to this, co-author of TinySec in 2003 offered a presentation on sensor networking security and reported that “Public-key cryptography is right out”. But in another time (2005), the same author states that “New reality: Public-key is no big deal”. This indicates the perception of people, regarding the use of public-key

cryptography, has been changed over time. Yet, we should accept the fact that this technique is highly expensive and requires more capability to enlarge the sensors life span.

In order to completely use public-key cryptography in WSN, it is essential to develop a public-key infrastructure (PKI) [Watro et al., 2004; Roma et al., 2007] which should be more reliable and trustworthy. But authors [Roma et al., 2007] suggest that the development of PKI is not essential for WSN specifically allotting signed certification of public-keys of various sensors may be difficult in several situations. For example, Liu and Bake et al. study in 2010 proposed *online/offline identity based* signatures for WSN which offers multi-time utility of the offline storage on contrary with MicaZ platform, one time usage scheme.

Another cryptographic algorithm is Hash function, otherwise called as message digests. It is one-way encryption algorithm which uses no key. Instead of key, it employs fixed-length hash value that can be computed based on the plain text, which makes the technique to be harsh to recover either content or the plain text length. Generally, hash algorithm is used to deliver a digital finger print of data often used to validate the reliability of data. Various operating systems employ hash function to encode passwords which provide a measure of file reliability and veracity. For example, study by Later, Shamir and Tauman [2001] introduced a novel technique namely "hash-sign-switch" in order to design more effective offline/online signature scheme. Unfortunately, both schemes failed to provide actual results and not effective too. Apart from this, there are several authors' implemented new online/offline schemes [Joye, Boneh, & Boyen, 2008; Kurosawa & Schmidt-Samoa, 2006]. Of these, scheme proposed by [Kurosawa and Schmidt-Samoa, 2006; Joye (2008] has proven safe and secure without random oracles, whereas scheme proposed by [Boneh & Boyen, 2008] has found to be more effective and efficient. But it should be noted that all schemes are applicable only for conventional public-key settings.

NEW TRENDS

The Role of Elliptic Curve Cryptography

The importance of *Elliptic Curve Cryptography* (ECC) was individually proposed by Koblitz [1987] and Miller in the year 1985. Presently, *Elliptic Curve Cryptography* has attained the attraction of many people as an efficient technique in providing security solution for wireless networks because of its low computation and small size. Using public-key cryptography as a key approach, and works based on the algebraic structure of elliptic curves over finite fields. As compared with traditional public key cryptography such as RSA, eclipse curve cryptography attains better result in providing security services. For instance, the security level of ECC having160-bit key length has found to be equal with RSA having 1024-bit key length [Joppe et al., 2009]. Alternatively, ECC has multiple operations that aid to provide more feasible results on sensor mote and it takes only 0.81 *second* on 8-bit CPU Atmel ATmegal128 MHz [Gura et al., 2001]. Despite, there are several ways to enhance the ECC operation. For example, Mutual Authentication and Access Control based on Elliptic Curve Cryptography (MAACE) a public key cryptography based ECC was proposed by Le, Khalid, Sankar and Lee (2011) for wireless sensor network in healthcare domain. The final outcome of the research reported that this novel protocol was light weight, more scalable and requires very minimal memory comparing with symmetric based cryptography. Other researchers such as Yeh et al., (2011) projected a secured authentication protocol using ECC for WSNs and reported its suitableness and reliability for greater security WSNs.

However, the main demerit of ECC is that it enhances the encrypted message size compared to RSA encryption. Moreover, the implementation of ECC is highly complex than RSA and also increases the implementation errors and thus decreasing algorithm security.

Quantum Cryptography

This technique provides modes for two parties in order to interchange an enciphering key through private channel in a complete communication security. Quantum cryptography is of three types for key distribution of networks. It includes:

A. Cryptosystems with encoding based on two non-commuting observables [Wiesner, 1970; Bennett & Brassard, 1984]
B. Cryptosystems with encoding built upon quantum entanglement [Ekert, 1990]
C. Cryptosystems with encoding based on two non-orthogonal state vectors [Bennett, 1992]

RECOMMENDATIONS AND CONCLUSION

WSN has become increasingly popular and highly employed in various applications. Thus, developing highly secure system or networks has become imperative but it is very challenging to develop such system as WSN possess only limited resources in terms of storage capacity, memory, and processing capability and so on. Apart from this, private issues are also an important problem in WSN which should be taken into consideration. Hence, it is essential to develop novel security algorithm or protocol to confront these problems. Cryptography is one such technique to confront security problems in WSN. However cryptography alone is not enough to confront WSN problems. In addition, public-key cryptography is highly expensive and ECC offers better performance benefits but being multilevel approach, the viable solution has obtained only in a combined form for securing system such as designing protocols, data aggregation, localization with regards to security principles. Overall, it is essential to use the key management process carefully in order to achieve higher security system networks.

REFERENCES

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002) 'A Survey on Sensor Networks', IEEECommunications Magazine, 40(8), 102-114.
[2] J. Liu, J. Baek, J. Zhou, J. W. Wong, "Efficient online/offline identity-based signature for wireless sensor network", *Journal International Journal of Information Security*, Vol. 9, No. 4, 2010.
[3] A. Bharathidasan, V. Anand, S. Ponduru, Sensor Networks: An Overview, Department of Computer Science. University of California, Davis, Technical *Report*, 2001.
[4] B. R. J. Caro, D. Garrido-Márquez, P. Plaza-Tron, R. Castro, J. L. Serrano-Martín, J. L, "SMEPP: A Secure Middleware for Embedded P2P", *In ICT Mobile and Wireless Communications Summit (ICT-MobileSummit'09)*, pp. 1-8, 2009.
[5] J. Lopez, Zhou, J, *Wireless sensor network security*. Amsterdam: Press, 2008.

[6] N. Sastry, and D. Wagner, "Security Considerations for IEEE 802.15.4 Networks", In *Proceedings of ACM Workshop on Wireless Security*, Philadelphia, PA, USA, 2003.

[7] H. L. Yeh, T. H. Chen, and H. W. Wei, "A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography", *Sensors*, vol. 11, no. 5, pp. 4767-4779, 2011.
[8] C. Karlof, N. Sastry, D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks", In *Proc. ACM SenSys '04*, ACM, Baltimore, pp. 162–175, 2004.
[9] A. Perrig, J. Stankovic, D. Wagner, "Security in wireless sensor networks", *Commun ACM.*, Vol. 47, No. 6, pp. 53–57, 2004.
[10] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, D. E. Culler, "SPINS: security protocols for sensor networks", Wireless Networks Journal, Vol. 8, No: 5, pp. 521–534, 2002.
[11] M. Beller, Y. Yacobi, "Fully-edged two-way public key authentication and key agreement for low-cost terminals", *Electronics Letters*, Vol. 29, No. 11, 1993.
[12] A. Biryukov, D. Wagner, "Slide attacks, in: International *Workshop* on Fast Software Encryption, 1999.
[13] J. Kohl, C. Neuman, The Kerberos network authentication service (V5), RFC 1510, 1993.
[14] Z. Haas, M. Perlman, "The ZoneRouting Protocol (ZRP)for ad hoc networks, Internet draft, Mobile Ad-Hoc Network (MANET) *Working Group*, IETF, 1998.
[15] G. Gaubatz, J.P. Kaps and B. Sunar, Public key cryptography in sensor networks – revisited, in: *First European Workshop on Security in Ad-hoc and Sensor Networks (ESAS)*, LNCS 3313, Springer, 2004, pp. 2–18.
[16] A. Wander, N. Gura, H. Eberle, V. Gupta, S. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks", In *Proc. PerCom '05*, *IEEE Computer Society*, New York, 2005.
[17] N. Gura, A. Patel, H. Wander, H. Eberle, S. Chang-Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs", :In *6th International Workshop on Cryptographic Hardware and Embedded Systems (CHES'04)*, LNCS 3156, Springer, pp. 119–132, 2004.
[18] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, P. Kruus, "Tinypk: Securing sensor networks with public key technology", In *Proc. 2nd ACM workshop on Security of ad hoc and sensor networks*, Washington, DC, 2004.
[19] R. Roma, C. Alcaraz, "Applicability of public key infrastructures in wireless sensor networks. In: Proc. EuroPKI '07", *Lecture Notes in Computer Science*, vol. 4582, pp. 313–320, 2007.
[20] A. Shamir, Y. Tauman, "Improved Online/Oine Signature Schemes", In *Proc. CRYPTO'01*, vol. 2139, pp. 355–367.
[21] M. Joye, "An efficient on-line/off-line signature scheme without random oracles. In: Proc. CANS '08", *Lecture Notes in Computer Science*, vol. 5339, pp. 98–107, 2008.
[22] K. Kurosawa, K. Schmidt-Samoa, "New online/offline signature schemes without random oracles. In: Proc. PKC '06", *Lecture Notes in Computer Science*, vol. 3958, pp. 330–346, 2006.
[23] D. Boneh, X. Boyen, "Short signatures without random oracles the SDH assumption in bilinear groups", *J. Cryptol*., Vol. 2, pp. 149–177, 2008.
[24] V. Miller, "Use of elliptic curves in cryptography", *CRYPTO*, Vol. 85, 1985.
[25] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, Vol. 48, pp. 203–209, 1987.
[26] W. Joppe, M. Kaihara, T. Kleinjung, A. K. Lenstra, P. Montgomery, On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography Cryptology, *Report* on Cryptology ePrint Archive, Vol. 389, 2009.

[27] N. Gura, A. Patel, A. Wander, H. Eberle, S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-it CPUs", *CHES*, Vol. 3156, pp.119-132, 2004.
[28] X. H. Le, M. Khalid, R. Sankar, S. Lee, "An Ecient Mutual Authentication and Access Control Scheme for Wireless Sensor Networks in Healthcare", *Journal of Networks*, Vol. 6, No. 3, pp: 355-364, 2011.
[29] S. Vanstone, "Next generation security for wireless: elliptic curve cryptography", *Computers & Security*, Vol. 22, No. 5, pp. 412–415, 2003.
[30] S. Wiesner, SIGACT *News* 15, 78(1983); original manuscript written circa 1970.
[31] C. H. Bennett, Brassard, G. *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing*. New York: IEEE, 19894.
[32]A. K. Ekert, "Physics Review Letter", Vol. 67, pp. 661, 1991.
[32] C. H. Bennett, "Physics Review", *Letter*, vol. 68, pp. 3121, 1992.