ISSUES AND CHALLENGES IN WSN SECURITY

Vandana[1], ReetiKamboj[2]

Department of Electronics & Communication Engineering
Maharishi VedVyas Engineering College, Jagadhri, India

Abstract-Sensor networks often provide services in hostile environments, which make them targets for malicious attacker. However, several features of sensor networks make it very challenging to provide security in sensor networks. Security plays a fundamental role in many wireless sensor network applications. Because sensor networks pose unique challenges, security techniques used in conventional networks cannot be directly applied to WSNs because of its unique characteristics. First, sensor nodes are very sensitive of production cost since sensor networks consist of a large number of sensor nodes. Second, Sensor nodes may be deployed in public hostile locations, which make sensor nodes vulnerable to physical attacks by adversaries. There are several mechanism through which security can be provided to the network. Some techniques consume huge energy to provide a high security and some consumes less energy but compromise the security of network. So we need to identify a mechanism which considers these facts. So the balanced security is a paramount factor for the success of wireless sensor networks. This paper presents a survey related to security issues in routing algorithm.

I. INTRODUCTION

Security plays a fundamental role in many wireless sensor network applications. Because sensor networks pose unique challenges, security techniques used in conventional networks cannot be directly applied to WSNs because of its unique characteristics. First, sensor nodes are very sensitive of production cost since sensor networks consist of a large number of sensor nodes. Energy consumption becomes a key consideration for most sensor network protocols. Second, Sensor nodes may be deployed in public hostile locations, which make sensor nodes vulnerable to physical attacks by adversaries. Sensor networks use insecure wireless communication channel and lack infrastructure. As a result, existing security mechanisms are inadequate, and new approaches are desired. This paper presents a security scenario in wireless sensor network.

II. SECURITY IN LEACH PROTOCOL[Heinzlman2002]

Wireless sensor networks consist of small nodes that sense their environment, process data, and communicate through wireless links. They are expected to support a wide variety of applications, many of which have at least some requirements for security. Cryptographic algorithm for authentication and encryption can be implemented in two ways: using public keys or private keys. When using public keys, the key value of every node is public information, and is therefore known by all other nodes. When a node wants to communicate privately with another node, the source node simply encrypts data using the public key of the sink node. In this case, only the sink node can correctly decrypt the data. This method is called asymmetric key encryption because the two communicating nodes use different keys during the session.When using private keys, nodes must first agree on a key before they can communicate securely. One possibility is to use public keys to encrypt data from which private keys can be derived. Private Key algorithms are based on symmetric key encryption because both communicating nodes use the same keys for encrypting and decrypting data. In wired data networks, nodes rely on pre-deployed trusted server to help establish trust relationships but in WSN, these trusted authorities do not exist because sensor nodes have limited memory, CPU power, and energy, hence

ISSN: 2278 – 909X

cryptographic algorithms must be selected carefully.In a sensor mote a small amount of resources are left for security to be implemented. This is insufficient to even hold the variables for asymmetric public key based cryptographic algorithms like RSA and Diffie-Hellman. Thus public key based systems do not work for sensor networks. Because of the resource constraints another solution is to use global keys. This is feasible but a global key based system does not provide the desired level of security. On the contrary, complete pair-wise keying between nodes provides the best possible security, but it is not a choice for sensor network because of the resource constraints.

The simplest method of key distribution is to preload a single network-wide key into all nodes before deployment. Only one single key is stored in the nodes' memory and once deployed in the network, there is no need for a node to perform key discovery or key exchange since all the nodes in communication range can transfer messages using the key which they already share. On the other hand, this scheme suffers a severe drawback that compromise of a single node would cause compromise of the entire network through the shared key. Thus it fails in providing the basic secure requirement of a sensor network by making it easy for an adversary trying to attack.An alternative key distribution scheme is fully pairwise keys scheme, i.e., every node in the sensor network shares a distinct key with every other node in the network. The main problem with this pairwise key scheme is its poor scalability. The number of keys that must be stored in each node is proportional to the total number of nodes in the network. Since sensor nodes are resource-constrained, this brings significant overhead which limits the scheme's applicability except for it can only be effectively used in smaller networks.The method of Kerberos-like key distribution is popular in a lot of networks environment. In sensor networks, we can use a trusted, secure base station as an arbiter to provide link keys to sensor nodes. The sensor nodes authenticate themselves to the base station, after which the base station generates a link key and sends it to both parties securely. An example of such a protocol is SNEP, a part of the SPINS security infrastructure. However, this kind of schemes suffers high energy consumption, which makes it inapplicable in most of sensor network applications. A detail discussion and research initiatives taken in the past decade have been presented in the next chapter.

III. LITERATURE REVIEW

Ensuring a good level of security for WSN is not a trivial task. As WSNs use wireless communications, the threats and attacks against them are more diverse and often large-scale. It is not possible to deal with all types of security threats with a single mechanism. Rather, a combination of different security schemes for a single network could be the solution. Several mechanisms at different layers can be employed simultaneously, to provide holistic security [Pathan2006] for wireless sensor networks and in addition the level of security in the data transmission and communication phase can be increased via efficient key management schemes. Public key cryptography (PKC) can be the best choice for ensuring a satisfactory level of security for data transmissions in the network. However, the major challenge of employing any public key-based security scheme in WSN is the constrained energy, computational, and memory budgets of sensors participating in the network. Because of this fact, PKC-based schemes were not utilized in these networks for quite some time.

To counter the bias against PKC for WSNs, several public key schemes have recently demonstrated an acceptable performance for low-power sensor nodes [Malan2004] [Wander2005] [Jing2006]. Many recent works have suggested the feasibility of PKC in WSNs, with little energy cost. This could be especially helpful in applications that require a high level of security. Several recent works have successfully implemented public key schemes with current-generation sensors. In terms of both software and

ISSN: 2278 – 909X

hardware perspectives, PKC schemes have shown reasonable performance. [Liu2008] presented the first known implementation of elliptic curve cryptography over F2p for sensor networks based on eight-bit, 7.3828 MHz MICA2 motes [Xbow2004]. The results show that a public key based scheme is feasible for current-generation sensors. The TinyPK system demonstrated in [Watro2004] shows that a public-key based protocol is feasible, even for an extremely lightweight sensor network. TinyPK is a software-based implementation of a public key system tested on UC Berkeley MICA2 motes.

Gaubatz et al. [Gaubatz2005] proposed a custom hardware-assisted approach which makes public key cryptography feasible in WSN environments, provided that suitable algorithms and associated parameters, careful optimization, and low-power design techniques are selected. In order to validate their claim, they present proof of concept implementations of two different algorithms; Rabin's Scheme and NtruEncrypt. Their work demonstrates that in spite of common assumptions about public key cryptography, it is possible to achieve a level of power consumption that is sufficiently low to enable its use even for battery-attached sensor nodes.In [Gaubatz2005a] it was shown that special purpose, ultra-low power hardware implementations of public key algorithms can be used for sensor nodes. The authors show that PKC tremendously simplifies the implementation of many typical security services and reduces transmission power, because of a lower protocol overhead. Also, [Gaubatz2005a] provides an in-depth comparison of three different PKC implementations (Rabin's scheme, NtruEncrypt, and Elliptic Curve) particularly aimed at wireless sensor networks.

Blab and Zitterbart [Blab2005] presented an efficient and lightweight implementation of public-key cryptography algorithms relying on elliptic curves. They checked their codes by implementing them on popular eight-bit ATMEGA128 microcontroller, the heart of the MICA2 platform. Their work concluded that public-key cryptography is feasible for sensor networks.Gupta et al. [Gupta2005] showed that elliptic curve cryptography not only makes public-key cryptography feasible for these devices, but also enables the creation of a complete, secure web server stack that runs efficiently with very stringent resource constraints. In [Wander2005], the authors conducted a comparative energy analysis of RSA and ECC based public key algorithms for wireless sensor networks. They use a simplified version of SSL for mutual authentication and key exchange. Murphy et al. [Murphy2006] showed that it is possible to implement public key algorithms for resource constrained sensor node platforms. Via a hardware/software co-design approach, they successfully map a public key cryptosystem based on Rabin's scheme.

Piotrowski et al. [Piotrowski2006] investigated four types of nodes; MICA2DOT, MICA2, MICAz, and TelosB, and estimated the power consumption for most common RSA and ECC operations. Their work gives an indication of how public key cryptography influences a wireless node's lifetime. In [Jing2006], the authors propose C4W, which is basically an identity-based PKC infrastructure. They show that their identity-based scheme consumes less energy, as it is certificate-less, and thus it is efficient, both in terms of computational and communication costs.A hardware implementation of PKC for elliptic curves over binary extension fields was proposed in [Bertoni2006]. In this paper, the authors proposed a dedicated coprocessor for certain cryptographic operations. They showed that a reasonable amount of power savings can be achieved in this case, and thus improved performance can be achieved, without degrading other performance parameters. A distributed, cooperative public key authentication scheme is proposed in [Nyang2006].

In [Mykletun2006] there was an examination of several additive homomorphic public key encryption schemes and their applicability to WSNs, when implemented on computationally limited sensor devices. The authors in this work provide recommendations for selecting the most suitable public key schemes based on topologies and scenarios for wireless sensor networks.In their works, Roman and Alcaraz[Roman2007] discussed the applicability of public key infrastructures to wireless

ISSN: 2278 – 909X

sensor networks and Ugus et al. [Ugus2007] implement elliptic curve and finite field arithmetic operations on a MICAz mote, which is a typical device employed in wireless sensor networks.

Other than the aforementioned works, in [Du2005], Du et al. suggest limited use of PKC, due to its high power consumption characteristics, and propose the use of a one-way hash function instead of a certificate. Construction of a Merkle tree forest from sensors' public keys and selection of the height of the tree are the basics of their scheme. They compare their scheme with other popular PK (public key) schemes for sensor networks, and plot the results, which show significant gains. However, the drawback of this scheme is that it requires storing some information in the sensors' memory, prior to their deployment.

Gaubatz, Kaps and Sunar [Gaubatz2004] first challenged the basic assertion of public key cryptography infeasibility in sensor networks, which are based on a traditional software based approach. They propose a custom hardware assisted approach for which they claim that it makes public key cryptography available in such environments, provided they use the right selection of algorithms and associated parameters, careful optimization, and low-power design techniques. In the family of public key algorithms, Elliptic Curve Cryptosystem (ECC) and Hyper Elliptic Curve Cryptosystem (HECC) are widely thought of as the best balance in terms of speed, memory requirement and security level. Malan, Welsh, and Smith [Malan2004] presented the first implementation of elliptic curve cryptography over GF(2p) for sensor networks based on the 8-bit, 7.3828MHz MICA2 mote.

Hu and Evans [Hu2003] proposed a secure hop-by-hop data aggregation scheme. In their scheme, individual packets are aggregated in some pattern so that the base station can detect unauthorized inputs. Jadia and Muthuria [Jadia2004] extended the Hu-Evans scheme. Instead of relying on keys shared between the base station and sensor nodes for authentication, Jadia-Muthuria scheme make use of one-hop as well as two-hop pairwise keys. It is intended to replace the data validation step of the Hu-Evans scheme with some other mechanism that does not require unnecessary key reception by all nodes. Yang, et al. [Yang2006] proposed SDAP, a secure hop-by-hop data aggregation protocol for sensor networks, using the principles of divide-and-conquer and commit-and-attest. In SDAP, a novel probabilistic grouping technique is utilized to dynamically partition the nodes in a tree topology into subtrees. A commitment-based hop-by-hop aggregation is conducted in each subtree to generate a group aggregate. The base station identifies the suspicious subtrees based on the set of group aggregates. Finally, each subtree under suspect participates in an attestation procedure to prove the correctness of its group aggregate. Feng et al. [Feng2008] proposed a family of secret perturbation-based schemes that protect sensed information confidentiality without disrupting the data aggregation.

Several secure aggregation algorithms have been proposed under the scenario that there are a certain classes of nodes called aggregators. Przydatek, Song, and Perrig [Przydatek] proposed secure information aggregation (SIA) to identify forged aggregation values from all sensor nodes in a network. In SIA scheme, aggregators compute an aggregation result over the raw data together with a commitment to the data based on a Merkle-hash tree and send data to a trustable remote user, who later challenges the aggregators to verify the aggregation. They assumed that the bandwidth between a remote user and aggregators is a bottleneck in this scenario. Therefore the SIA scheme is intended to reduce this communication overhead while providing a mechanism to detect with high probability if aggregators are compromised.Homomorphic encryption [Fontaine20007] is semantically-secure encryption which, in addition to standard guarantees, has additional properties, e.g. the sum of any two encrypted values is equal to the encrypted sum of the values. There are several efficient homomorphic cryptosystems, such as Unpadded RSA, El-Gamal, Goldwasser-Micali, Benaloh and Paillier [Fontaine20007]. Using homomorphic encryption, Kifayat et al. [Kifayat2007] presented the extended structure and density

ISSN: 2278 – 909X

independent group based key management protocol (SADI-GKM) with the additional feature of secure data aggregation to provide better data confidentiality to every single node in a large scale wireless sensor network. Ren, Kim, and Park [Ren2007] also proposed a secure data aggregation scheme which supports end-to-end encryption using homomorphic encryption as well as hop-by-hop verification using ECC based MAC.

IV. ISSUES AND CHALLENGES IN SECURE WSN

Encryption and key distribution are important primitives to build secure Wireless Sensor Networks (WSN). Different block ciphers were proposed in literature to provide encryption in resource constraint distributed networks. A large amount of different key distribution schemes were implemented, targeting different types of WSNs. These schemes face issues with respect to their requirements, implementations, and theoretic foundations. Though security is regarded as a standalone component of the architectures of many systems, in case of wireless sensor networks, it must get adequate attention. The types of services expected in wireless sensor networks often require the network security architecture. In most application domains, the sensors are used to collect a specific type of data from particular target areas, and the collected data are often considered secret and are not intended for public disclosure. Hence, efficient and secure mechanisms are needed to transmit acquired data securely to the appropriate recipients.

In security schemes based on symmetric cryptography, when a node is compromised, the adversary can get the secret keys stored in it and personate other nodes who have shared secret keys with the compromised node to forge messages. Random key distribution approaches are prevailing at present. However, few analyses about communication overload in these schemes have been conducted. Especially, finding a secure path in a random graph is a NP-complete problem. Most of those schemes just ignored this problem. Rekey and perfect backward secrecy are also serious issues for those random pre-distribution schemes. How the compromised nodes affect the security of the whole networks is therefore a main factor for evaluation. As a public key cryptosystem, the security of private keys is certainly the focus. The common perception of public key cryptography is that it is complex, slow, power hungry, and not at all suitable for use in ultra-low power environments like wireless sensor networks. To keep energy consumption low, nodes have limited computing power, small RAM, and low storage capacity. Thus, classic public key cryptography based on RSA trapdoor function is not suitable due to its high computational overhead. The complexity of RSA operations does not scale linear with their key size, which makes them too costly when initialized with parameters defined as sufficiently secure by the National Institute of Standards and Technology or other standard institutions1. As today's key management schemes heavily rely on public key cryptography, researchers have proposed several lightweight alternatives to RSA based key management. Once keys are exchanged and authenticated, efficient block ciphers are required to encrypt network communication in real time. Besides block ciphers, which were designed for a small memory footprint and smaller block size, modern microcontrollers used in sensor nodes come with implementations of the Advanced Encryption Standard (AES). From the practical point of view, group key distribution and public key based might be the tendency. The progress in efficiently implementation of Elliptic Curve Cryptosystem (ECC) and Hyper Elliptic Curve Cryptosystem (HECC) and advances in sensor hardware will make public key cryptosystem practicable in a few years. Many applications in the area of Wireless Sensor Networks (WSN) would gain a lot from the availability of strong public key cryptography (PKC). The most important advantage is the availability of authentication and key exchange mechanisms that are more secure and reliable compared to secret key cryptography. However, besides the advantages, the public key cryptography has also one main disadvantage. It is

ISSN: 2278 – 909X

computationally expensive. It is nowadays clear that it is possible to apply it but the question that remains is how the application of strong public key cryptography affects the lifetime of the energy source and thus the lifetime of the sensor. That is why here we try to investigate the costs of public key cryptography in WSN and their influence to the node lifetime.

It is not easy to judge whether the PKC is generally too expensive for WSN or not. The verdict depends on many application specific factors, e.g., how often In many applications of wireless sensor networks, the base station is more interested in aggregated data than exact individual values from all sensors. By aggregating data, it is also greatly helpful to reduce the amount of data to be transmitted for conserving valuable energy. Indeed, current in-network aggregation schemes are beneficial to communication energy consumption but they are designed without considering possible security issues. Furthermore, wireless sensor networks are often designed with neighbor nodes sharing keys or with decryption at aggregator nodes. In either situation the potential for aggregator nodes to be physically compromised means that data confidentiality is at high risk. Therefore secure data aggregation is desirable where data can be aggregated without the need for decryption at aggregator nodes. Aggregation becomes especially challenging if end-to-end confidentiality between a source and a destination is required. Current proposed secure data aggregation schemes are rather elementary and more practical schemes are demanded. It is worthwhile to pay more attention how to apply homomorphic encryption to secure aggregation effectively. In the meantime, it is of great help to focus on specific popular aggregation protocols of WSNs to design realistic secure aggregation.

As WSNs grow in application area and are used more frequently, the need for security in them becomes inevitable and vital. However, the inherent characteristics of WSNs incur constraints to of sensor nodes, such as limited energy, processing capability, and storage capacity, etc. These constraints make WSNs very different from traditional wireless networks. Consequently, many innovative security protocols and techniques have been developed to meet this challenge.

CONCLUSION

In this paper we outline security and privacy issues in sensor networks, address the state of the art in sensor network security and energy consumption of different scheme; specially application of public key cryptography also known as homomorphic encryption. Till now it is a known fact that asymmetric key cryptography is not suitable for WSN. But with the introduction of new energy efficient sensor nodes such as telosB etc.,researchers are exploring and evaluating the effect of public key cryptography on WSN. They are also exploring the use of new hybrid encryption scheme for providing effective security environment with low energy consumption.Based on the literature survey and above discussion we can say that homomorphic encryption provides a better security as compared to secret key cryptography (SKC) can be employed in WSN scenario where we need to protect our data during communication and also in aggregation phase. However it may consume more power than SKC. It will also remove the requirement of key distribution which is a major headache in SKC.

REFERENCES

[Bertoni2006] Bertoni, G., Breveglieri, L., and Venturi, M., “Power Aware Design of an Elliptic Curve Coprocessor for 8 bit Platforms,” *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops* (*PERCOMW’06*), p. 337, 2006.

ISSN: 2278 – 909X

[Blab2005] Blab, E. O. and Zitterbart, M., "Towards Acceptable Public-Key Encryption in Sensor Networks," *Proceedings of ACM 2nd International Workshop on Ubiquitous Computing*, Miami, USA, pp. 88-93, May 2005.

[Du2005] Du, W., Wang, R., and Ning, P., "An Efficient Scheme for Authenticating Public Keys in Sensor Networks," Proceedings of ACM MobiHoc'05, Illinois, USA, 2005, pp. 58-67.

[Feng2008] T. Feng, C. Wang, W. Zhang, and L. Ruan. Confidentiality Protection for Distributed Sensor Data Aggregation. In IEEE The 27th Conference on Computer Communications (INFOCOM 2008), pages 56–60, 2008.

[Fontaine20007] C. Fontaine and F. Galand. A survey of homomorphic encryption for nonspecialists. EURASIP Journal on Information Security, 2007(1):1–15, 2007.

[Gaubatz2004] G. Gaubatz, J.-P. Kaps, and B. Sunar. Public key cryptography in sensor networksrevisited. In 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS-2004), 2004.

[Gaubatz2005] Gaubatz, G., Kaps, J.-P., and Sunar, B., "Public Key Cryptography in Sensor Networks-Revisited," *ESAS 2004*, *LNCS 3313*, Springer-Verlag, pp. 2-18, 2005.

[Gaubatz2005a] Gaubatz, G., Kaps, J.-P., Ozturk, E., and Sunar, B., "State of the Art in Ultra-Low Power Public Key Crytography for Wireless Sensor Networks," *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 146-150, 2005.

[Gupta2005] Gupta, V., Wurm, M., Zhu, Y., Millard, M., Fung, S., Gura, N., Eberle, H., and Shantz, S. C., "Sizzle: A Standards-based End-to-End Security Architecture for the Embedded Internet," *SMLI TR-2005-145*, June 2005.

[Heinzelman2002] W. B. Heinzelman, A. P. Chandrakasan and H. Balakrishnan.An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications,* vol. 1, no. 4, pp. 660- 670, 2002.

[Hu2003] L. Hu and D. Evans. Secure aggregation for wireless networks. In Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), pages 384 – 391, 2003.

[Jadia2004] P. Jadia and A. Mathuria. Efficient Secure Aggregation in Sensor Networks. In High Performance Computing (HiPC 2004), pages 40–49. LNCS 3296, 2004.

[Jing2006] Jing, Q., Hu, J., and Chen, Z., "C4W: An Energy Efficient Public Key Cryptosystem for Large-Scale Wireless Sensor Networks," *Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems* (*MASS*), pp. 827-832, Oct. 2006.

[Kifayat2007] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones. Applying Secure Data Aggregation techniques for a Structure and Density Independent Group Based Key Management Protocol. In Third International Symposium on Information Assurance and Security (IAS 2007), pages 44–49, 2007.

[Liu2008] A. Liu and P. Ning. TinyECC: A Configurable Library for Elliptic Curve Cryptographyin Proc. 7th International Conference on Information Processing in Sensor Networks (IPSN 2008), pp. 245–256, 2008.

[Malan2004] D. J. Malan, M. Welsh, and M. D. Smith.A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON 2004), pages 71–80, 2004.

[Malan2004] Malan, D.J., Welsh, M., and Smith, M.D., "A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography," *Proceedings of IEEE SECON 2004*, pp. 71-80, 4-7 October, 2004.

[Murphy2006] Murphy, G., Keeshan, A., Agarwal, R., and Popovici, E., "Hardware - Software Implementation of Public-Key Cryptography for Wireless Sensor

ISSN: 2278 – 909X

Networks," *Proceedings of Irish Signals and Systems Conference*, pp. 463-468, 28-30 June 2006.

[Mykletun2006] Mykletun, E., Girao, J., and Westhoff, D., "Public Key Based Cryptoschemes for Data Concealment in Wireless Sensor Networks," *Proceedings of IEEE International Conference on Communications*, pp. 2288-2295, 2006.

[Nyang2006] Nyang D. and Mohaisen A., "Cooperative Public Key Authentication Protocol in Wireless Sensor Network," *UIC 2006*, *LNCS 4159*, Springer-Verlag, pp. 864-873, 2006.

[Pathan2006] Pathan, A.-S. K., Lee, H.-W., and Hong, C. S., "Security in Wireless Sensor Networks: Issues and Challenges," *Proceedings of 8th IEEE ICACT 2006*, Volume II, 20-22 February, Phoenix Park, Korea, pp. 1043-1048, 2006.

[Piotrowski2006] Piotrowski, K., Langendoerfer, P., and Peter, S., "How Public Key Cryptography Influences Wireless Sensor Node Lifetime," *Proceedings of ACM SASN 2006*, Virginia, USA, pp. 169-176, 2006.

[Ren2007] S. Q. Ren, D. S. Kim, and J. S. Park.A Secure Data Aggregation Scheme for Wireless Sensor Networks. In Frontiers of High Performance Computing and Networking ISPA 2007 Workshops, pages 32–40. LNCS 4743, 2007.

[Roman2007] Roman, R. and Alcaraz, C., "Applicability of Public Key Infrastructures in Wireless Sensor Networks," *EuroPKI 2007*, *LNCS 4582*, Springer-Verlag, pp. 313-320, 2007.

[Ugus2007] Ugus, O, Hessler, A., and Westhoff, D., "Performance of Additive Homomorphic EC-ElGamal Encryption for TinyPEDS," Technical Report 6, July 2007, available at: http://www.ist-ubisecsens.org/publications/EcElgamal-UgHesWest.pdf

[Wander2005] Wander, A.S., Gura, N., Eberle, H., Gupta, V., and Shantz, S.C., "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," *Proceedings of PerCom'05*, pp. 324-328, 2005.

[Watro2004] Watro, R., Kong, D., Cuti, S.-f., Gardiner, C., Lynn, C. and Kruus, P., "TinyPK: Securing Sensor Networks with Public Key Technology," *Proceedings of ACM SASN'04*, Washington, DC, USA, pp. 59-64, 2004.

[Xbow2004] Xbow Sensor Networks, available at: http://www.xbow.com/

[Yang2006] Y. Yang, X.Wang, S. Zhu, and G. Cao. A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks. In Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing, pages 356 – 367, 2006.

ISSN: 2278 – 909X