Overview of Security Research in EYES

Yee Wei Law Pieter Hartel Sandro Etalle Paul Havinga
University of Twente, The Netherlands
Email: {ywlaw, pieter, etalle, havinga}@cs.utwente.nl

Roberto di Pietro Luigi Mancini
University of Rome “La Sapienza”, Italy
Email: {dipietro, mancini}@di.uniroma1.it

The security research for the EYES project is mainly carried out by the the University of Rome “La Sapienza” and the University of Twente. While Rome is primarily interested in key management, Twente has been involved with an assortment of topics such as key management, cryptographic primitives and link-layer security. This document gives an overview of the research output of these two groups for the past 3 years.

Security in wireless sensor networks (WSNs) is a wide area. In the course of trying to cover as many important issues as possible, we have only looked at what we think are the most basic of all issues, from a software point of view. This document is intended to give an overview of these very basic issues (Figure 1).

This document is organized as follows:

Section I is dedicated to our assessment of the general assumptions that are applicable to the security of WSNs.

Section II describes our evaluation of cryptographic primitives, for the purpose of selecting the appropriate primitives to be used for sensor networks.

Section III details the work we have done in key management. This is the area we have spent the most research effort in because key management is crucial to the proper working of cryptographic security mechanisms.

Section IV is about security on the data link layer.

Section V covers some work we have done in intrusion response.

Section VI gives some concluding remarks about our results, some afterthought and some ideas about where we should be heading in our future research agenda.

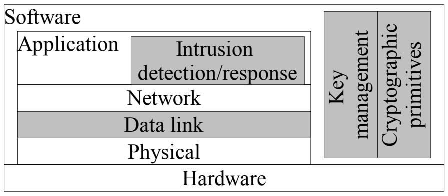

Fig. 1. Focus areas (shaded regions) of security research in EYES.

I. Security profile

It is often the case that when technology precedes its applications (as is the case with WSNs), the assumptions on which the technology is built on are murky. We have set out to clarify these assumptions in one of our SEC 2003 papers [1]. We profile the security requirements/assumptions of a system by a set of what we term the boolean-valued *critical system parameters*:

1) message confidentially (MC): *all* messages need to be encrypted;
2) tamper-resistance (TR): sensor node hardware is tamper-resistant;
3) public-key cryptographic capability (PKCC): sensor nodes are capable of executing public-key cryptographic algorithms;
4) Rich Uncles (RU) [2]: there are nodes in the network that are significantly more resource-rich than most of the others.

The type of WSNs we are aiming at in EYES falls under the profile where MC=0, TR=0, PKCC=0, RU=1 (contrary to our original idea that MC=1, TR=0, PKCC=1, RU=1). This gives us a starting point for designing our security architectures.

II. Evaluation of cryptographic primitives

The energy efficiency requirement of WSNs is especially important because the sensor nodes are meant to operate without human intervention for a long period of time with little energy supply. Besides, available storage is scarce due to their small physical size. Therefore choosing the most storage- and energy-efficient block cipher for WSNs is important. However to our knowledge so far, no systematic work has been conducted in this area. In our MASS 2004 paper [3], we have identified the candidates of block ciphers suitable for WSNs based on existing literature and authoritative recommendations. We have benchmarked these candidates and based on this benchmark, we have selected the suitable ciphers for WSNs, namely Rijndael (i.e. AES) for high security and energy efficiency requirements; but MISTY1 for good storage and energy efficiency. In terms of operation mode, we recommend Output Feedback (OFB) mode for static networks, but Counter mode for dynamic networks.

The recommendation of MISTY1 as an alternative to AES might come as a surprise, but it is actually recommended by NESSIE [4] (as a legacy cipher) and CRYPTREC [5]. As for our vote for OFB/Counter mode instead of the more popular choice of CBC [6], our explanation is as follows: CBC not only requires lost blocks to be re-transmitted, but also requires more code, data memory and CPU cycles. CBC is popular in the wired world only because unlike other modes, the re-use of initialization vectors can be tolerated, but this benefit is outweighed by the need for re-transmissions.

III. Key management

The quality of a secure architecture not only depends on the security of the underlying encryption or authentication primitives but also on how the keys are managed. *Key management* is the set of processes and mechanisms which support key establishment and the maintenance of ongoing keying relationships between parties, including replacing older keys with new keys (*key refreshment*) as necessary [7]. *Key establishment* is any process whereby a shared secret key becomes available to two or more parties, for subsequent cryptographic use [7].

A. LKH++

One of our first proposals is LKH++ [8], a key management scheme for multicast (a form of group communication). This paper [8] presents an efficient algorithm for the secure group key management of mobile users. The most promising protocols to deal with group key management are those based on the logical key hierarchy (LKH) model. The LKH model reduces the resources needed to logarithmic size: computation time, the number of messages exchanged, and memory space. In the framework of the LKH model, we present a new protocol LKH++ that outperforms the other proposed solutions in the literature. Such performance improvements are obtained by exploiting both the properties of one-way hash functions and the information that the users already share in the LKH model. In particular, when a user eviction occurs in LKH++, each remaining user autonomously constructs a new key along the path from the evicted user to the root as a function of a specific logical child key. Therefore, the center can carry on the re-keying phase by distributing only a subset of the new keys and by reducing the number of communications to the users. When a join occurs, minimal information is broadcast, while most of the communications are unicast toward just the joining user. The proposed LKH++ protocol establishes a group communication of n users requiring to unicast $((n-1)\log n)/2$ keys, while standard algorithms require to deliver $n\log n$ keys. Our solution allows the users to form promptly a new group if the wireless ad hoc network needs to be reconfigured. Moreover, the proposed extension to deal with mass leave and mass join allows a considerable savings in the messages sent by the center, as well as in the computations required by both the center and the users. Finally, the LKH++ protocol enhances the reliability of key management due to the reduced number of communications needed in the re-keying phase.

B. LKHW

LKH++ does not take into account the peculiarities of WSNs. LKHW has been proposed to take advantage of the in-network processing capability of WSNs [9]. Like LKH++, LKHW is an extension of LKH, but also merged with directed diffusion [10]. The resulting protocol, LKHW, combines the advantages of both LKH and directed diffusion: robustness in routing, and security from the tried and tested concepts of secure multicast. In particular, LKHW enforces both backward and forward secrecy, while incurring an energy cost that scales roughly logarithmically with the group size. This is the first security protocol that leverages directed diffusion, and we showed how directed diffusion can be extended to incorporate security in an efficient manner.

Apart from LKH++ and LKHW, a more general decentralized key management architecture for WSNs, covering the aspects of key deployment, key refreshment and key establishment, has been developed [11]. This architecture is based on a clear set of assumptions and guidelines. A balance between security and energy consumption is achieved by partitioning a system into two interoperable *security realms*: the *supervised realm* trades off simplicity and resources for higher security whereas in the *unsupervised realm* the opposite is true. Key deployment uses minimal key storage while key refreshment is based on the well-studied scheme of Abdalla et al [12]. The keying protocols involved use only symmetric cryptography and have all been verified with our constraint solving-based protocol verification tool CoProVe [13].

C. Random key pre-distribution

An interesting problem in key management is how to implement secure pair-wise communications among any pair of sensors in a WSN. A WSN requires completely distributed solutions which are particularly challenging due to the limited resources and the size of the network. Moreover, WSNs can be subjected to several security threats, including the physical compromising of a sensor. Hence, any solution for secure pairwise communications should tolerate the collusion of a set of corrupted sensors. A novel solution has been proposed by Eschenauer and Gligor [14]. The scheme is called *random key pre-distribution*. Following their breakthrough, we have added some improvements.

Our probabilistic model is based on Eschenauer and Gligor's [14]. In our model, two protocols (Direct Protocol and Co-operative Protocol) are used to establish a secure pair-wise communication channel between any pair of sensors in the WSN, by assigning a small set of random keys to each sensor [15]. The Co-operative Protocol allows the asserted level of security to be changed dynamically during the life-time of a WSN. Both protocols also guarantee implicit and probabilistic mutual authentication without any additional overhead and without the presence of a base station. The performance of the Direct Protocol has been analytically characterized while, for the Co-operative Protocol, we have provided both analytical evaluations and extensive simulations. For example, the results show that, assuming each sensor stores 120 keys, in a WSN composed of 1024 sensors with 32 corrupted sensors the probability of a channel corruption is negligible in the case of the Co-operative Protocol.

We have also addressed the problem of connectivity in Secure Wireless Sensor Networks (SWSN) using the scheme of random key pre-distribution, by using a geometric random model [16]. Under this new and realistic model, we describe how secure and connected networks using a small constant number of keys per sensor can be constructed. Our result, supported by extensive simulations, demonstrates how connectivity can be guaranteed for a wide interval of practical network sizes and sensor communication ranges.

D. Performance tweaking

Our work in increasing the performance of key management for secure multicast is best represented by one of our papers in SEC 2003 [17]. We propose in the paper, a methodology for establishing the minimal key length that guarantees a specified level of confidentiality [17]. We reach such a result by analyzing and extending the threat model to the confidentiality of the multicast information. For this extended threat model, we present a methodology that takes into account the following parameters: (1) the required lifetime of the information confidentiality; (2) the level of the key in the LKH model; (3) the dynamics of the multicast group, that is the eviction rate of the users. From these rationales we develop an analytical model that, for each level, derives the appropriate key length, that is the minimal length that ensures the desired degree of confidentiality under the hypotheses in the threat model. Finally, for a specific instance of the LKH model, we describe a numerical example that shows the saving that can be achieved in terms of the key lengths.

IV. Link-layer security

While it is definitely a possibility for attackers to compromise sensor nodes physically by tampering with the hardware, we see a more immediate threat in denying the service of WSNs by means of jamming. Blind radio jamming is straightforward to execute but not energy-efficient. We assume that an attacker has 2 goals: the primary goal is to disrupt the network by preventing messages from arriving at the sink node, and the secondary goal is to increase the energy wastage of the sensors. Furthermore, we imagine that the attacker wants to prolong these effects for as long as possible, hence the attacker needs to do it efficiently, and by choosing link-layer jamming, he can. This is the case because by exploiting the semantics of the link-layer protocol (aka MAC protocol), an attacker can achieve better efficiency than by blindly jamming the radio signals alone. In our EWSN 2005 paper [18], we investigate some jamming attacks on S-MAC [19], the level of effectiveness and efficiency the attacks can potentially achieve, and a countermeasure that can be implemented against one of these attacks.

The value we see in this work in that while there are a lot of security loopholes in today's WSN routing protocol [20], an attacker may find it far easier to launch DoS attacks by attacking the data link layer. Otherwise, the attacker would either have to tamper with the sensor node hardware, or implement a physical and data link layer compatible with the sensor nodes just to get to the network layer.

V. Intrusion response

Intrusion detection in WSNs has remained elusive despite some preliminary work done in this area [21], due to the simple fact that anomalies cannot easily be separated from the harsh operation environments WSNs are subjected to. We have however done some work in the area of intrusion response.

In particular, we propose an extension to the current WSN model (in particular the base station model), by introducing a Supervisor which has very few interactions with the network [22]. The Supervisor itself is mobile, could have more powerful hardware and it is asynchronous with respect to the sensors. Nevertheless, the Supervisor has to interact with the sensor network, for example to invoke the command to exclude from the network a selected sensor. We believe such a model is particularly suitable for, but not limited to, military applications. The model employs a distributed, cooperative and parallel algorithm to enforce the following properties: (1) the secure exclusion of a detected compromised sensor from the network, and (2) the re-keying of the remaining sensors. It has an overall low overhead both in terms of computation and required transmitted messages. It is scalable, since the algorithm requires only limited, local knowledge of the network topology. Finally, it can be adopted, as an independent layer, to enforce secure exclusion in other models.

VI. Conclusion

Experience shows that instead of absolute resistance, the security of WSNs is one that is based on *resilience* [23]. While the physical nature (not tamper-resistant, limited computational resources, limited power...) of sensor nodes does little to help with security, the nature of their operation, i.e. mobility [24] and redundancy offer many interesting opportunities. For the simplest example, data can be routed *around* the area of the network that is jammed. In our future work, we will continue to take advantage of these opportunities, and extend our investigation to secure routing and secure data aggregation [25].

References

[1] Y. Law, S. Etalle, and P. Hartel, "Assessing security in energy-efficient sensor networks," in *18th IFIP TC11 International Conference on Information Security, Security and Privacy in the Age of Uncertainty (SEC 2003)*, D. Gritzalis, S. D. C. di Vimercati, P. Samarati, and S. Katsikas, Eds. Kluwer Academic Publishers, May 2003, pp. 459–463. [Online]. Available: http://wwwhome.cs.utwente.nl/~ywlaw/pub/law03assessing.pdf

[2] D. Carman, P. Kruus, and B. Matt, "Constraints and approaches for distributed sensor network security," NAI Labs, Tech. Rep. #00-010, 2000. [Online]. Available: http://download.nai.com/products/media/nai/zip/nailabs-report-00-010-final.zip

[3] Y. Law, J. Doumen, and P. Hartel, "Benchmarking block ciphers for wireless sensor networks (extended abstract)," in *1st IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS 2004)*. IEEE Computer Society Press, Oct. 2004. [Online]. Available: http://wwwhome.cs.utwente.nl/~ywlaw/pub/law04benchmarking.pdf

[4] *Portfolio of recommended cryptographic primitives*, NESSIE Consortium, Feb. 2003.

[5] CRYPTREC, "電子政府推奨暗語の仕様書(trans.: Specification of e-government-recommended ciphers)," Web page, Dec. 2003. [Online]. Available: http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/cryptrec20030425_spec01.html

[6] C. Karlof, N. Sastry, and D. Wagner, "Tinysec: A link layer security architecture for wireless sensor networks," in *Second ACM Conference on Embedded Networked Sensor Systems (SensSys 2004)*, Nov. 2004.

[7] A. Menezes, S. Vanstone, and P. V. Oorschot, *Handbook of Applied Cryptography*. CRC Press, Inc., 1996.

[8] R. D. Pietro, L. Mancini, and S. Jajodia, “Efficient and secure keys management for wireless mobile communications,” in *Proc. 2nd ACM Int. Workshop on Principles of Mobile Computing*. ACM Press, 2002, pp. 66–73.

[9] R. D. Pietro, L. Mancini, Y. Law, S. Etalle, and P. Havinga, “LKHW: A directed diffusion-based secure multicast scheme for wireless sensor networks,” in *32rd International Conference on Parallel Processing Workshops (ICPPW ’03)*, C.-H. Huang and J. Ramanujam, Eds. IEEE Computer Society Press, Oct. 2003, pp. 397–406. [Online]. Available: http://wwwhome.cs.utwente.nl/~ywlaw/pub/dipietro03lkhw.pdf

[10] C. Intanagonwiwat, R. Govindan, and D. Estrin, “Directed diffusion: A scalable and robust communication paradigm for sensor networks,” in *6th Annual Int. Conf. on Mobile Computing and Networking (MobiCOM ’00)*. Boston, Massachusetts, United States: ACM Press, 2000, pp. 56–67.

[11] Y. Law, R. Corin, S. Etalle, and P. Hartel, “A formally verified decentralized key management architecture for wireless sensor networks,” in *4th IFIP TC6/WG6.8 International Conference on Personal Wireless Communications (PWC 2003)*, ser. LNCS, M. Conti, S. Giordano, E. Gregori, and S. Olariu, Eds., vol. 2775. Springer-Verlag, Sept. 2003, pp. 27–39. [Online]. Available: http://wwwhome.cs.utwente.nl/~ywlaw/pub/law03formally.pdf

[12] M. Abdalla and M. Bellare, “Increasing the lifetime of a key: A comparitive analysis of the security of rekeying techniques,” in *Advances in Cryptology – ASIACRYPT 2000*, ser. LNCS, T. Okamoto, Ed., vol. 1976. Springer-Verlag, 2000, pp. 546–565. [Online]. Available: http://www.cs.ucsd.edu/users/mihir/papers/rekey.html

[13] R. Corin and S. Etalle, “An improved constraint-based system for the verification of security protocols,” in *9th Int. Static Analysis Symp. (SAS)*, M. Hermenegildo and G. Puebla, Eds., vol. 2477. Madrid, Spain: Springer-Verlag, Sep 2002, pp. 326–341.

[14] L. Eschenauer and V. Gligor, “A key-management scheme for distributed sensor networks,” in *Proc. 9th ACM conference on Computer and communications security*. ACM Press, 2002, pp. 41–47.

[15] R. D. Pietro, L. Mancini, and A. Mei, “Random key assignments for secure wireless sensor networks,” in *1st ACM Workshop on Security of Ad-hoc and Sensor Networks*. ACM Press, Oct. 2003, pp. 62–71. [Online]. Available: http://cesare.dsi.uniroma1.it/Sicurezza/doc/sasn2003.pdf

[16] R. D. Pietro, L. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, “Connectivity properties of secure wireless sensor networks,” in *2nd ACM workshop on Security of ad hoc and sensor networks*. ACM Press, 2004, pp. 53–58.

[17] R. D. Pietro, L. Mancini, and A. Mei, “A time driven methodolgy for keys dimensioning in secure multicast communications,” in *Security and Privacy in the Age of Uncertainty. 18th IFIP Int. Information Security Conf.*, D. Gritzalis, S. D. C. di Vimercati, P. Samarati, and S. Katsikas, Eds. Kluwer Academic Publishers, 2003, pp. 121–132.

[18] Y. Law, P. Hartel, J. den Hartog, and P. Havinga, “Link-layer jamming attacks of S-MAC,” in *2nd European Workshop on Wireless Sensor Networks (EWSN ’2005)*. IEEE Communications Society, 2005.

[19] W. Ye, J. Heidemann, and D. Estrin, “Medium Access Control with Coordinated, Adaptive Sleeping for Wireless Sensor Networks,” *IEEE/ACM Transactions on Networking*, vol. 12, no. 3, pp. 493–506, 2003. [Online]. Available: http://www.isi.edu/~weiye/pub/smac_ton.pdf

[20] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” *Elsevier’s Ad Hoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, vol. 1, no. 2–3, pp. 293–315, 2003. [Online]. Available: http://www.cs.berkeley.edu/~daw/papers/

[21] Y. Zhang and W. Lee, “Intrusion detection in wireless ad-hoc networks,” in *6th Annual ACM/IEEE International Conference on Mobile Computing (MOBICOM’00)*, 2000, pp. 275–283.

[22] R. D. Pietro, L. Mancini, and S. Jajodia, “Secure selective exclusion in ad hoc wireless network,” in *Security in the Information Society: Visions and Perspectives*, M. Ghonaimy, M. El-Hadidi, and H. Aslan, Eds. Kluwer Academic Publishers, 2002, pp. 423–434.

[23] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” *Commun. ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[24] S. Čapkun, J.-P. Hubaux, and L. Buttyán, “Mobility helps security in ad hoc networks,” in *MobiHoc ’03: Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*. ACM Press, 2003, pp. 46–56.

[25] D. Wagner, “Resilient aggregation in sensor networks,” in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*. ACM Press, 2004, pp. 78–87.