Annales UMCS Informatica AI __, _ (____) _–_
DOI: __.____/______-___-____-_

Annales UMCS
Informatica
Lublin-Polonia
Sectio AI

http://www.annales.umcs.lublin.pl/

Energy-aware Key Management in Mobile Wireless Sensor Networks

Xiaobing He[1*], Pawel Szalachowski[2†], Zbigniew Kotulski[2‡], Nikos Fotiou[3§],
Giannis F. Marias[3¶], George C. Polyzos[3‖], Hermann de Meer[1**]

[1] *Faculty of Computer Science and Mathematics, University of Passau, Passau, Germany.*

[2] *Institute of Telecommunications, the Faculty of Electronics and Information Technology, Warsaw University of Technology, Warsaw, Poland.*

[3] *Department of Informatics, Athens University of Economics and Business, Athens, Greece.*

Abstract – Wireless sensor networks have received wide attention recently across indoor and outdoor applications. One the other hand, more and more application scenarios require sensor nodes to be mobile, which introduces new technological challenges for security. Key management is the core for secure data communications among resource-constrained sensor nodes. In this paper, based on Group Diffie-Hellman key agreement protocols and the energy level of each node in the network, we propose Energy Aware Group Diffie-Hellman key management protocols for mobile wireless sensor networks. Simulation results show that the proposed key management protocols provide a great improvement in maximizing the lifetime of networks.

---

[*] hebing@fim.uni-passau.de

[†] p.szalachowski@stud.elka.pw.edu.pl

[‡] zkotulsk@tele.pw.edu.pl

[§] fotiou@aueb.gr

[¶] marias@aueb.gr

[‖] polyzos@aueb.gr

[**] demeer@uni-passau.de

1 Introduction

A Wireless Sensor Network (WSN) consists of a large number of battery powered sensor nodes, equipped with sensing, data processing and short-range radio communication components [**1**]. WSNs have a wide range of applications, including agricultural, industrial, military and health monitoring systems. WSNs present unique security challenges compared to wire and ad hoc networks, such as the usage of the wireless medium, limited processing capabilities of sensor nodes and the absence of physical protection. This situation becomes more complicated when mobility is added to nodes. The node mobility make WSN applications become smarter and create new applications [**2**]. However, the unique characteristics of Mobile Wireless Sensor Networks (MWSNs) present a new set of nontrivial challenges in terms of open network architecture, resource constraints and highly dynamic change of network topology [**3**].

In MWSNs, a particularly important challenge is the creation of an end-to-end secure channel between remote nodes. Thus, key management is of paramount importance for MWSNs. A number of key management schemes have been proposed in the literature [**4, 5**]. However, some of them are considered suitable only for static WSNs and tend to be application-specific, while others introduce significant storage cost and computational overhead. It is a common belief that public-key protocols are unsuitable for sensor nodes due to the fact that public key algorithms such as RSA are computational intensive and usually execute thousands or even millions of multiplication instructions to perform a single-security operation [**6**]. However, recent studies have shown that public key cryptography such as Elliptic Curve Cryptography (ECC) [**7**] and Rabin's scheme [**8**] might be feasible in sensor networks. One of the most common public key protocols is Diffie-Hellman key agreement protocol [**9**].

This paper revisits and modifies a set of Group Diffie-Hellman (GDH) protocols, in order to attain energy efficient group key management in MWSNs. To achieve this goal, we propose Energy Aware Group Diffie-Hellman (EAGDH), a key management protocol that takes into consideration the energy level of nodes and distributes the computational burden of key generation accordingly.

The rest of the paper is organized as follows. Section 2 provides related work in this area as well as motivation for our work. Section 3 reviews Group Diffie-Hellman based key distribution. Section 4 presents our key management solution, while in Section 5 the simulation results are analyzed. Finally, we conclude this paper with future work in Section 6.

2 Related work, motivation and notations

2.1 Related work

Although there are numerous key management approaches (such as [**10, 11, 12**]) for WSNs, they cannot be applied in MWSNs, as they are under the assumption that the deployed nodes are stationary. Therefore, new key management approaches for MWSNs are required. Chuang et al.[**13**] proposed a two-layered dynamic key management (TDKM) scheme for mobile and long-lived cluster based wireless sensor networks. In TDKM, both pair-wise key and group key are distributed in three rounds without any encryption/decryption and exponentiation operation. Khan et al.[**14**] presented a runtime key management scheme for mobile heterogeneous sensor networks that consist of mobile sensor nodes and few fixed sensor nodes. Blundo et al.[**15**] proposed polynomial-based key pre-distribution scheme for mobile sensor networks. Kifayat et al.[**16**] proposed a group-based key management scheme which uses distinct keys at different levels in the network, while Aileni et al.[**17**] examined efficient ways of key distribution among sensor nodes and inter/intra-communications.

2.2 Motivation

MWSNs have the benefit over traditional static sensor networks in that they can deal better with changing operational conditions (e.g., node failure, battery depletion of some nodes) provide better network coverage and supply more accurate intrusion detection. Because of the mobility of nodes in the network, WMSNs can be better applies in building fire emergency response, target tracking and dairy cattle health monitoring. In future ubiquitous environments each wireless sensor node may be mobile in nature [**18**]. However, mobility introduces vulnerabilities to adversaries [**16, 19**]. As nodes are moving from one place to the other, node authentication, communication confidentiality and data integrity must be ensured.

On the other hand, sensor nodes are constrained in energy supply and bandwidth, and moreover, mobile entities require additional power for mobility. Thus, new security protocols specifically designed for MWSNs should take energy awareness as an essential consideration. Key management can be considered as a fundamental requirement for securing sensor networks upon which other security primitives are built. A large portion of node's energy is spent for generating and distributing cryptographic keys to mobile nodes, especially when its join/leave rate is very high. As key management schemes have not been designed with energy awareness in mind, they can not always be directly applied in energy-constrained MWSNs without firstly been reconsidered and modified. This paper is a step towards this direction.

2.3 Notations

Table 1 shows the notations appear in the rest of this paper.

3 Group Diffie-Hellman key distribution

Diffie-Hellman (DH) key exchange protocol [**20**] is a widespread solution used by most popular cryptographic schemes. Classic DH solves key exchange problem between two parties communicating over an insecure communication channel. However, it has two major disadvantages: firstly, it is relatively slow because it is realized by modular

Table 1. Notations

CH	cluster head
n	number of nodes (participants) in one cluster
i,j,k	indices of group members (ranging in [1,n])
e_i	energy level of i-th node
e_i^{act}	actual battery capacity of i-th node
e_i^{max}	maximum battery capacity of i-th node
M_i	the i-th node of one group
N_i	secret value of the i-th node
G	base-point of the Elliptic Curve
p	a primer
C_i	energy cost of a regular node i
n_m^i	number of multiplications executed by node i
n_s^i	number of messages sent by node i
n_r^i	number of messages received by node i
C_m	cost of a single multiplication computation
C_s^i	cost of sending one single message
C_r^i	cost of receiving one single message
C_{RX}	reception consumption
C_{TX}	transmission consumption
tbr	transmit bit rate
m	mean (average) number of execution
σ	standard deviation
v	variation ratio
γ_1	asymmetry (skewness) coefficient
γ_2	excess (kurtosis) coefficient

exponentiations and the key in this case is relatively long; secondly, the key exchange process is dedicated only to two parties. An extension of DH to group setting was first studied in [**21**], where three variants of Group Diffie-Hellman (GDH) protocols were presented. The basic scheme is described in the rest of this section.

We consider Elliptic Curve (EC) encryption, as the keys in EC is relatively shorter for providing the same level of security [**7**]. All EC parameters, other than N_i, are assumed to be secure and known to all participants. The basic Group Diffie-Hellman is defined as shown in Protocol 1.

GDH consists of two stages: upflow (traffic flows from the group member with low index to that with high index, as shown in the first stage of the protocol) and downflow

Protocol 1: Elliptic-Curve-based Group Diffie-Hellman

```
1: $M_i \longrightarrow M_{i+1} : \{\prod_{k=1}^{j}(N_k)G \mid j \in [1,i]\}$
2: $M_{n-i} \longleftarrow M_{n-i+1} : \{\prod_{k \notin [i,j]}(N_k)G \mid j \in [1,i]\}$
```

(the opposite of upflow, as shown in the second stage of the protocol). The protocol needs $2(n-1)$ messages, $i+1$ multiplications for $M_i(1 \leq i \leq n-1)$ and n multiplications for M_n. In the first stage, the size of messages increases on each link, whereas it decreases in the second stage. Furthermore, GDH does not need synchronization or broadcasting ability.

It should be noticed that in all GDH variants, there is no priori sequencing and numbering of group members, which means the index of one group member (whether *n-2* or n)is assigned arbitrarily in real time, as the protocol executes.

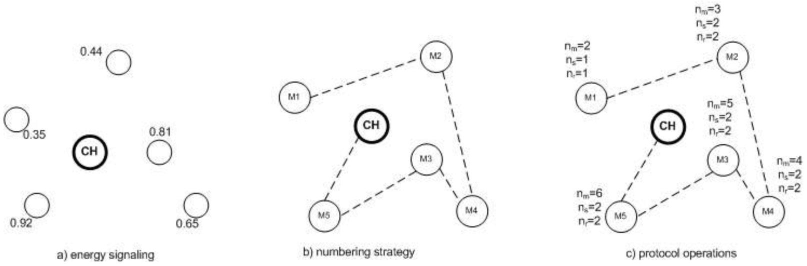
Security of GDH protocols is related to the security of DH protocol. GDH is secure as long as DH is secure. The protocols' details (execution, security proof, performance and other capabilities) can be found in [**21**].

4 Energy-aware Group Diffie-Hellman key management

4.1 Assumptions

It is assumed the network is split into clusters based on nodes' physical location and it is composed of three types of nodes. The base station (BS) is a data requester and serves as the gateway to the Internet. In general, BS is supplied with unlimited energy, high computation power and sufficient storage capacity. CHs are special nodes which compared to regular nodes have more energy, higher computational and processing capabilities as well as more storage capacity. Regular nodes can move from one cluster to another, and they are responsible for sending the data sensed from the surrounding area to the BS through CHs. There are two roles in our key management scheme, Group Leaders (GLs) and Group Members (GMs). In one cluster, a CH serves as a GL and all member mobile nodes serve as GMs. The proposed solution relies on the following assumptions:

(1) The maximum distance between any two GMs in the cluster is the communication range of the sensor.
(2) A sensor node could not be recharged if its energy is exhausted.
(3) Each sensor node has an unique identifier.
(4) The communication channels are bidirectional; if a node M_i can receive a message from node M_j, then M_i can send a message to M_j.
(5) The cost for sending one single message and for receiving one single message is the same.
(6) CHs can communicate directly with the BS.



a) energy signaling b) numbering strategy c) protocol operations

FIG. 1. Example of EAGDH execution

4.2 System overview

In GDH protocols, it can be observed that the last node (the node with the highest index) M_n in one group plays a special role: in all GDH variants, M_n performs the most number of multiplications. In our network setup, we assume that CH plays the role of the highest-indexed node M_n and there are $n-1$ regular nodes in one cluster.

Our goal is to make GDH energy aware such that the maximum number of protocol's execution is guaranteed. Our purpose is to reduce energy consumption on exhausted nodes (or nodes with lower energy level) by reducing the amount of computation overhead required to compute a cryptographic key. As nodes ordering affects the protocol's execution effort on a given node, we take advantage of no priori ordering attribute of GDH protocols. In our EAGDH, CH is the node with the highest-index. CH receives the energy level of each GM and decides the index for each GM. This phase of EAGDH is called numbering strategy. By making use of energy factors: C_m, C_s^i and C_r^i, energy consumption of EAGDH for a regular node can be expressed as:

$$C_i = n_m^i C_m + n_s^i C_s^i + n_r^i C_r^i. \tag{1}$$

The selections of GDH protocol and numbering strategy mainly depend on the size of the cluster as well as those energy factors. The value of each factor is strictly connected with hardware platforms. Some platforms can perform communication procedures (sending and receiving) in a very efficient way, while others have high computational processing power. Table 2 presents the number of operations performed on a regular node M_i in one cluster. The table does not include the operations of the CH (M_n) as CH is assumed to be more resource-powerful node.

TABLE 2. Number of operations performed on a regular node in a cluster

	GDH
messages sent	2, 1 for M_1
messages received	2, 1 for M_1
multiplications	$i+1$

An energy efficient variant of GDH is presented in Protocol 2. An execution example of the protocol, named EAGDH, is shown in Fig. 1. The objective of EAGDH is to let the more exhausted nodes perform the fewer operations.

```
Protocol 2: Energy Aware Group Diffie-Hellman
1: Each node $x$ within a cluster sends its energy level $e_x$ with its identifier to GL.
2: GL orders nodes in increasing order of the energy level using given sorting
   algorithm.
3: GL assigns indices to each member corresponding to the order obtained in step 2.
4: GMs execute GDH.
```

5 Simulation and evaluation

In this section we evaluate the proposed schemes using two platforms: MICA2 and Tmote Sky, on which most ECC-based security schemes are based. A typical MICA2 node is equipped with an 8-bit ATmega128L microcontroller, 4Kb of RAM, 128Kb of Flash memory and CC1000 chip as a radio module. A Tmote Sky node is equipped with a 16-bit MSP430 microcontroller, 10Kb of RAM, 48Kb of Flash memory, and CC2420 chip is employed as the radio module. Here, the ECC implementation presented in [**22**] is employed.

The performance results of point multiplication (multiple additions of a point) are essential. In our simulation, we chose the most efficient case, where an EC is defined over prime-order field $\mathbb{F}_q$. An EC point is described by 160 bits, so in our protocol the messages' sizes are multiples of this value. Based on [**22**] and the platforms' datasheets, the required costs for different operations is presented in Table 3.

TABLE 3. Parameters for both platforms

Parameter	**MICA2**	**Tmote Sky**
C_{RX}	10.0mA	21.8mA
C_{TX}	25.0mA	19.5mA
tbr	$3.84e+04$ bps	$2.5e+05$ bps
C_m	$1.27s \times 7.88mA$	$0.72s \times 3.68mA$

For both platforms, we assume that the maximum battery's capacity (b_i^{max}) of all nodes is 3000 mAh. Our goal is to maximize the number of protocol executions in a group of n nodes. We examine three cases: the *worst* case, during which the ordering of nodes never change, the *mean* in which the set of nodes is permuted randomly after each execution and the *optimal* case in which after each execution the nodes are renumbered in the way presented in Protocol 2. To determine the number of protocol's executions, we simulated each case for 1000 times under various node densities and simulation stopped unless unless any one node runs out of its battery. To explain explicitly, we

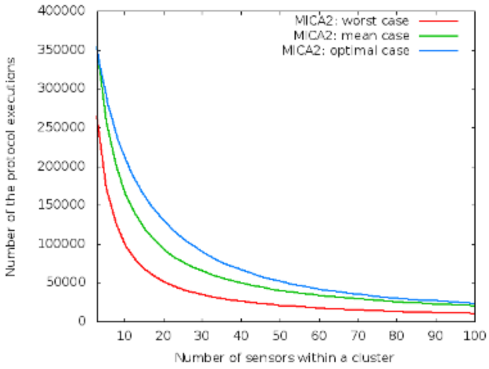


FIG. 2. Performance of EAGDH on MICA2 platform

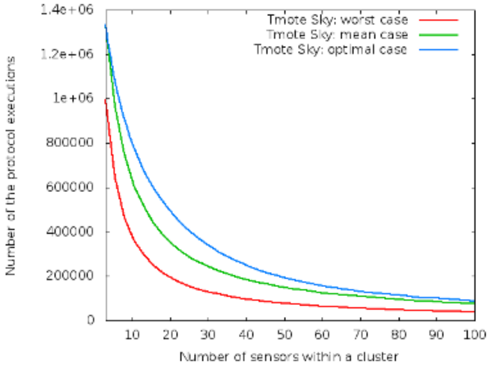


FIG. 3. Performance of EAGDH on Tmote Sky platform

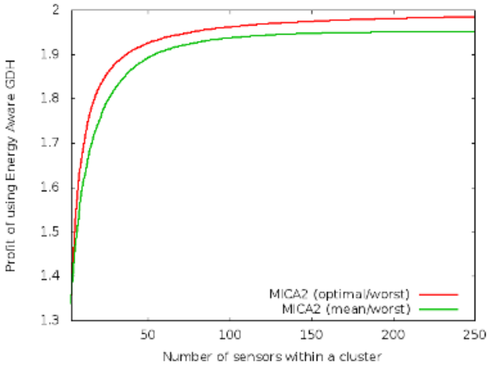


FIG. 4. Profits achieved on MICA2 platform

simulated the above mentioned three cases in one cluster, while others have the same

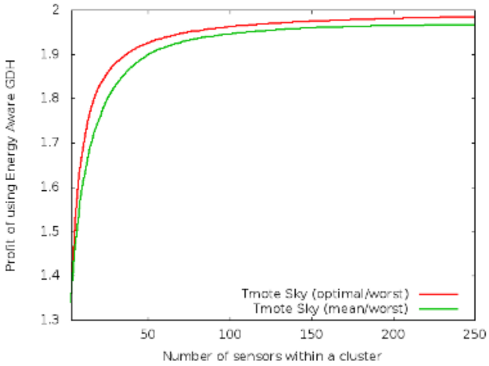


FIG. 5. Profits achieved on Tmote Sky platform

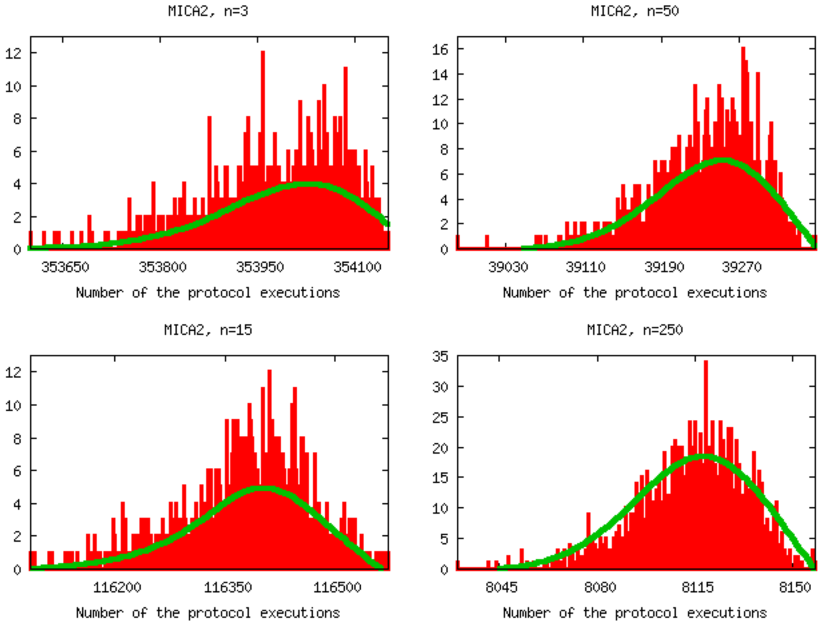


FIG. 6. Histograms of simulations for MICA2

attributes with this one. The simulation outcome for the MICA2 platform is presented in Fig. 2, while for Tmote Sky platform is presented in Fig. 3.

For MICA2, with a small number of n, the gap (measured as the number of the protocol's executions) is about 80000 executions. With the increase of n, the gap narrows but the relative advantage of using EAGDH is still growing.

In the case of Tmote Sky, the gap between the optimal case and the worst case is about 300000 executions. The mean case for both platforms starts with values near to

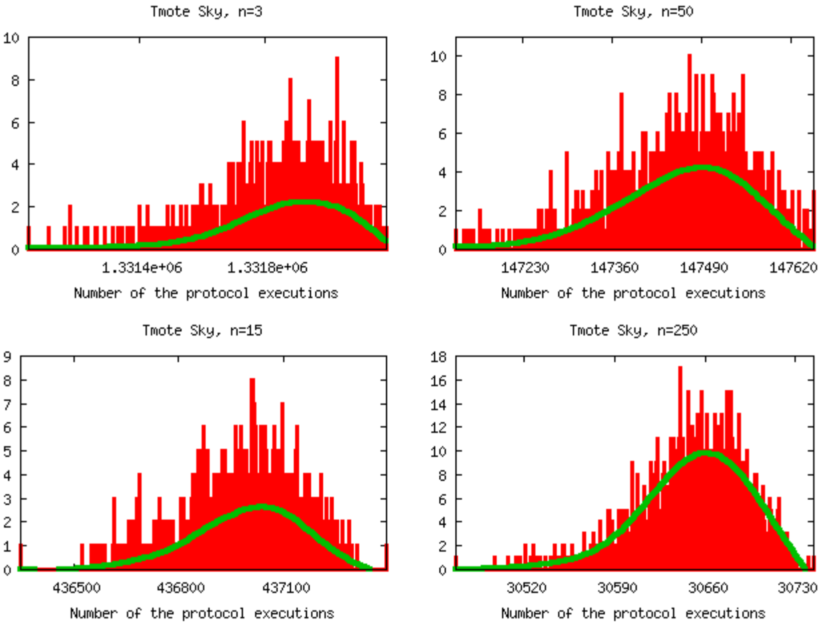


Fig. 7. Histograms of simulations for Tmote Sky

Table 4. Parameters of the mean case (MICA2)

n	**3**	**8**	**15**	**25**	**40**	**50**	**65**	**80**	**100**	**140**	**150**	**180**	**200**	**250**
$m \times 10^{-3}$	353	191	116	74	48	39	30	24	20	14	13	11	10	8
σ	99	103	81	66	55	51	41	38	33	28	27	24	23	19
$v \times 10^{-3}$	0.3	0.5	0.7	0.9	1.1	1.3	1.3	1.5	1.6	1.9	2	2.1	2.3	2.4
$-\gamma_1$	0.79	0.64	0.62	0.62	0.73	0.84	0.66	0.79	0.96	0.71	0.82	0.54	0.73	0.65
γ_2	0.41	0.29	0.49	0.75	0.49	0.93	0.58	1.50	2.93	0.55	1.12	0.34	0.9	0.61

that of the optimal one, but it approaches to the worst case and for $n \gtrsim 25$ it converges again to the optimal case. The simulation results of the mean case will be discussed in details and interpreted later.

Fig. **??** presents the profits achieved by using EAGDH on both platforms. For a given platform the profit is computed by dividing the number of protocol executions in the optimal case or in the mean case by that in the worst case. The simulation results show that both platforms (MICA2 and Tmote Sky) have almost the same rate in the optimal case (the red line in Fig. 4 and Fig. 5). In both figures, for the optimal case, the profit of using EAGDH increases rapidly with the increase of sensor nodes and converges to 2, which means that two times more protocol's execution can be achieved by using EAGDH compared to the worst case.

TABLE 5. Parameters of the mean case (Tmote Sky)

n	**3**	**8**	**15**	**25**	**40**	**50**	**65**	**80**	**100**	**140**	**150**	**180**	**200**	**250**
$m \times 10^{-3}$	1331	718	436	280	181	147	114	93	75	54	50	42	38	30
σ	188	189	149	130	103	94	84	71	63	55	50	46	43	40
$v \times 10^{3}$	0.14	0.26	0.34	0.47	0.57	0.64	0.73	0.76	0.83	1	1	1.1	1.1	1.3
$-\gamma_1$	0.99	0.87	0.51	0.68	0.74	0.58	0.82	0.59	0.65	0.84	0.61	0.72	0.80	0.77
γ_2	1.34	2.31	0.17	0.62	1.16	0.2	1.26	0.43	0.73	1.3	0.34	0.85	0.94	0.91

We now focus on the mean case. Before analyzing the simulation results, first we define and explain the coefficients needed in the probability density function. Variation ratio v is defined as a measure of dispersion which can be calculated as follows: $v = \frac{\sigma}{m}$. Moreover skewness coefficient is set as $\gamma_1 = \frac{\mu_3}{\sigma^3}$, where μ_3 is the central moment of third order. For a symmetric random variable, $\gamma_1 = 0$. For $\gamma_1 \neq 0$, the probability density function has a long tail at the right-hand side of the mean value (if $\gamma_1 > 0$) or a long tail at the left-hand side of the mean value (if $\gamma_1 < 0$). Finally, we set $\gamma_2 = \frac{\mu_4}{\sigma^4} - 3$, where μ_4 is the central moment of the fourth order. For the normal distribution, the kurtosis coefficient $\gamma_2 = 0$. If $\gamma_2 > 0$ then, the given probability density function is taller and its shape is slimmer around the modal value than the density of the normal distribution. While in the case of $\gamma_2 < 0$ the opposite is observed. Further description and interpretations of these parameters for them can be found in [**23**].

The results for the MICA2 platform are presented in Table 4 and Fig. 6, while the values for Tmote Sky are in Table 5 and Fig. 7. From these tables and figures, it is observed that the advantage of applying EAGDH over GDH in average is remarkable but not very high. However, higher moments of their distribution show that using EAGDH gives essential profits. The distribution has a long tail for short network lifetimes, namely, the probability of short lifetimes is very high (due to skewness's negative values which have relatively high absolute values). High probability of the values in the left-hand tail is confirmed by the positive value of kurtosis (Fig. 6 and Fig. 7). It can be seen that, in order to avoid network collapses, EAGDH should be used instead of GDH when nodes have consumed more than half of their batteries.

6 Conclusions and future work

In this paper, we proposed Energy Aware Group Diffie-Hellman key management protocols for mobile wireless sensor networks. By reducing computational burden on low energy level sensor nodes, EAGDH protocols help to extend the lifetime of a network. The simulation results show that, in realistic communication environment, our protocols are very energy efficient.

Future work includes the security analysis of the proposed key management protocols, particularly under diverse adversarial models, such as node capture attacks, node replication attacks and reply and modification attacks. Moreover a protocol extension that handles node addition and deletion shall be consider. Finally, the establishment of a secure channel between cluster head and the base station shall also be addressed in our next work.

Acknowledgment

The research leading to the results in this paper has been supported by the EuroNF SJRP. 54 E-Key-Nets project. Pawel's work is supported by the National Science Center (NCN), under Grant with decision's number DEC-2011/01/N/ST7/02995.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, pp. 102–114, 2002.

[2] S. A. Munir, B. Ren, W. Jiao, B. Wang, D. Xie, and J. Ma, "Mobile wireless sensor network: Architecture and enabling technologies for ubiquitous computing," in *Proceedings of AINA Workshops*, 2007.

[3] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," *IEEE Wireless Communications*, vol. 11, pp. 38–47, 2004.

[4] Y. Zhang, Y. Shen, and S. Lee, "A cluster-based group key management scheme for wireless sensor networks," in *12th International Asia-Pacific Web Conference (APWEB)*, 2010.

[5] G. Wang, S. Kim, D. Kang, D. Choi, and G. Cho, "Lightweight key renewals for clustered sensor networks," *Journal of Networks*, vol. 3, pp. 300–312, 2010.

[6] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks," *Wirel. Netw.*, vol. 8, no. 5, pp. 521–534, 2002.

[7] V. S. Miller, "Use of elliptic curves in cryptography," in *Lecture notes in computer sciences; 218 on Advances in cryptology—CRYPTO 85*. New York, NY, USA: Springer-Verlag New York, Inc., 1986, pp. 417–426.

[8] M. O. Rabin, "Digitalized signatures and public-key functions as intractable as factorization," Cambridge, MA, USA, Tech. Rep., 1979.

[9] D. Malan, M. Welsh, and M. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," in *First Annual IEEE Communications Sociery Conference on Sensor and Ad Hoc Communications and Networks*, 2004.

[10] H. Liang and C. Wang, "An energy efficient dynamic key management scheme based on polynomial and cluster in wireless sensor netwoks," *JCIT: Journal of Convergence Information Technology*, vol. 6, pp. 321–328, 2011.

[11] Y. Wang and B. Ramamurthy, "Group rekeying schemes for secure group communication in wireless sensor networks," in *IEEE International Conference on Communications*, 2007.

[12] C.-H. Park, Y.-Y. Zhang, I.-T. Kim, and M.-S. Park, "Dls: Dynamic level session key revocation protocol for wireless sensor networks," in *International Conference on Information Science and Application (ICISA)*, 2010.

[13] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Two-layered dynamic key management in mobile and long-lived cluster-based wireless sensor networks," in *IEEE Wireless Communications and Networking Conference*, 2007.

[14] S. Khan, L. Lavagno, C. Pastrone, and M. Spirito, "An effective key management scheme for mobile heterogeneous sensor networks," in *Internatioal Conference on Information Society (i-Society)*, 2011.

[15] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO '92. London, UK: Springer-Verlag, 1993, pp. 471–486.

[16] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones, "Group-based key management for mobile sensor networks," in *IEEE Sarnoff Symposium*, 2010.

[17] A. R. Aileni, "Key management in mobile sensor networks," *CoRR*, vol. abs/1104.2565, 2011.

[18] P.Kalyani and C. Chellappan, "Heterogenous wireless mobile sensor network model based routing adopted to dynamic topology," *European Journal of Scientific Research*, vol. 50, pp. 143–150, 2011.

[19] X. Deng and Y. Xiong, "A new protocol for the detection of node replication attacks in mobile wireless sensor networks," *Journal of Computer Science Technology*, vol. 26, pp. 732–743, 2011.

[20] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644–654, 1976.

[21] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-hellman key distribution extended to group communication," in *Proceedings of the 3rd ACM conference on Computer and communications security*, 1996.

[22] P. Szczechowiak, L. B. Oliveira, M. Scott, M. Collier, and R. Dahab, "Nanoecc: testing the limits of elliptic curve cryptography in sensor networks," in *Proceedings of the 5th European conference on Wireless sensor networks*, ser. EWSN'08, 2008.

[23] Z. Kotulski and W. Szczepiński, *Error Analysis with Applications in Engineering.* Springer, 2010.

[24] E. J. Duarte-melo and M. Liu, "Data-gathering wireless sensor networks: Organization and capacity," *Computer Networks*, vol. 43, pp. 519–537, 2003.

[25] N. Gura, A. Patel, A. WANDER, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and rsa on 8-bit cpus," in *Cryptographic Hardware and Embedded Systems-CHES 2004*, vol. 3156, 2004, pp. 119–132.

[26] M. Kalantary and M. Meybodi, "Energy-aware routing protocol for mobile sensor networks using learning automata algorithms," in *IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communicatrions (WiMob)*, 2010.

[27] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203–209, 1987.

[28] B. Ren, J. Ma, and C. Chen, "The hybrid mobile wireless sensor networks for data gathering," in *Proceedings of the 2006 international conference on Wireless communications and mobile computing*, ser. IWCMC '06, 2006.

[29] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1978.

[30] P. Szalachowski, B. Ksiezopolski, and Z. Kotulski, "On authentication method impact upon data sampling delay in wireless sensor networks," in *Computer Networks*, ser. Communications in Computer and Information Science, A. Kwiecień, P. Gaj, and P. Stera, Eds. Springer Berlin Heidelberg, 2010, vol. 79, pp. 280–289.

[31] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*, 2005.

[32] K. Xu, X. Hong, and M. Gerla, "An ad hoc network with mobile backbones," in *IEEE International Conference on Communications, ICC 2002.*, 2002.