Cryptography and Security Schemes for Wireless Sensor Network

Kriptografi dan Skema Keamanan untuk Jaringan Sensor Nirkawat

Taufiq Wirahman

Pusat Penelitian Informatika
Lembaga Ilmu Pengetahuan Indonesia
Gedung 20 lt 3, Jln Sangkuriang 154 D, Bandung
Indonesia

Abstract

This paper attempts to explore the security issues in sensor network that include constraints in sensor networks security, the requirements of secure sensor networks, attack classification and its counter measures and security mechanisms at wireless sensor network (WSN) such as cryptography and key management. Popularity of wireless sensor network is increasing because of its potential to provide low-cost solution for a variety of real-world problem. As a special form of ad-hoc networks, sensor networks has many limitations that lead to vulnerabilities in security issues. Currently, there are many researches in the field of sensor network security. Our analysis shows that symmetric key cryptography systems are more favorable to provide WSN security services because of its computation and energy cost. Moreover, distributed combine with pre-distributed key management is important to overcome security threats and centralize threats detection is more favorable to reduce energy and computation cost of sensor nodes.

Key Words: survey, wireless sensor network, security issues, cryptography, key management

Abstrak

Makalah ini berusaha untuk mengupas aspek keamanan pada jaringan sensor yang meliputi hambatan yang ada pada keamanan jaringan sensor, persyaratan yang diperlukan bagi jaringan sensor agar aman, klasifikasi serangan pada jaringan sensor dan pertahanan terhadap serangan yang terkait serta mekanisme keamanan yang ada pada jaringan sensor seperti kriptografi dan manajemen kunci. Popularitas jaringan sensor nirkawat semakin meningkat karena potensinya dalam menyediakan solusi berbiaya rendah bagi berbagai masalah dunia nyata. Sebagai bentuk khusus dari jaringan *ad-hoc*, jaringan sensor memiliki banyak keterbatasan yang menyebabkan kerentanan dalam masalah keamanan. Pada saat ini telah banyak riset dalam bidang keamanan jaringan sensor. Hasil analisis menunjukkan bahwa kriptografi kunci simetri lebih baik daripada yang lainnya untuk menyediakan layanan keamanan berdasarkan biaya komputasi dan energi yang dibutuhkan. Selain itu, manajemen kunci terdistribusi yang dikombinasikan skema kunci pre-distribusi dapat mengurangi kerentanan kegagalan keamanan dan sistem deteksi serangan lebih baik dalam bentuk terpusat dengan pertimbangan tidak memberatkan proses komputasi pada setiap simpul.

Kata kunci: survei, jaringan sensor nirkawat, keamanan, kriptografi, manajemen kunci

1. PENDAHULUAN

Jaringan sensor nirkawat (*wireless sensor network*, WSN) adalah suatu jaringan yang terdiri dari simpul yang dilengkapi dengan sensor bertenaga baterai yang terdiri dari komponen komputasi, pemroses data dan komunikasi [1], yang digunakan untuk mengindera, mengumpulkan informasi dan mengirimkan data yang diperoleh ke stasiun induk untuk diproses lebih lanjut [2]. Pada saat ini, popularitas WSN semakin menanjak karena kemampuannya untuk dapat diterapkan dalam berbagai bidang dengan biaya murah [3].

WSN mempunyai karakteristik unik yang membedakannya dengan jaringan biasa. Kemampuan komputasi dan komputasi WSN lebih terbatas dengan kapasitas memori dan

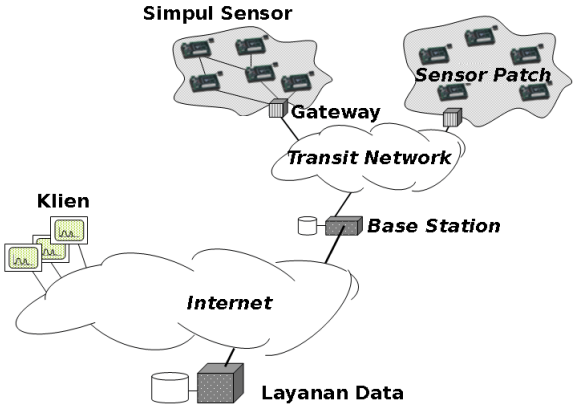
*Corresponding Author. Tel: +6222-2504711
Email: taufiq@informatika.lipi.go.id
Received: 4 Oct 2012; revised: 21 Oct 2012; accepted: 21 Nov 2012
Published online: 26 Nov 2012

daya yang terbatas pula [4]. Di samping itu, WSN biasanya dipasang pada lingkungan yang dapat diakses secara fisik sehingga meningkatkan potensi serangan secara fisik [5]. Meskipun WSN memanfaatkan teknik jaringan nirkawat, tetapi pendekatan keamanan untuk jaringan nirkawat tidak bisa diterapkan secara langsung pada WSN karena keunikan fitur dan kebutuhan aplikasinya [6].

Beberapa penelitian telah membahas tentang isu keamanan pada WSN seperti pada [3][4][5][6][7][8][9][10], akan tetapi perkembangan WSN yang begitu pesat membutuhkan ulasan yang lebih lanjut seiring banyaknya isu dan teknik keamanan baru yang ditawarkan. Pada makalah ini akan dipaparkan tentang aspek keamanan pada WSN yang meliputi hambatan yang ada pada keamanan WSN, persyaratan keamanan bagi jaringan sensor, klasifikasi serangan dan pertahanan terhadap serangan yang terkait. Akan dibahas juga tentang skema keamanan jaringan sensor yang meliputi kriptografi, manajemen kunci, deteksi dan pencegahan serangan serta *routing*.

2. ASPEK KEAMANAN WSN

Suatu WSN adalah bentuk khusus dari jaringan *ad-hoc* [4] yang mempunyai beberapa perbedaan dan keterbatasan di beberapa sisi. Gambaran arsitektur sistem WSN seperti terlihat pada Gambar 1 [11].



Gambar 1. Arsitektur Sistem WSN

Terkait dengan keamanan ada beberapa pertimbangan yang perlu diperhatikan yaitu:

(1) Keterbatasan sumber daya, diantaranya memori, ruang penyimpanan dan daya [8][10]. Dengan keterbatasan tersebut, ukuran kode algoritma keamanan simpul harus dibatasi. Sedangkan semakin rumit tingkat komputasi kode akan memakan energi semakin besar.

(2) Ketidakandalan komunikasi, yang meliputi ketidakandalan transfer, konflik antar paket dan latensi [8]. Penggunaan protokol *peerless* dan pengaruh kesalahan kanal dapat menyebabkan paket menjadi cacat. Kemacetan jaringan, *routing* multi hop dan keberadaan simpul pemroses akan memacu latensi yang lebih besar pada jaringan yang menyebabkan sulit tercapainya sinkronisasi antar simpul.

(3) Operasi jaringan tanpa pengawasan dimana WSN ditempatkan pada kawasan terpencil yang mudah untuk dieksploitasi secara fisik dan pengendalian sensor dari jarak jauh berakibat deteksi gangguan secara fisik lebih sulit [8][10].

2.1 Persyaratan Keamanan

Dalam WSN, persyaratan keamanan dapat diklasifikasikan sebagai berikut [4][6][8][10][12]:

(1) Kerahasiaan, dimana informasi tidak dapat diakses oleh pihak yang tidak berwenang.

(2) Integritas, yang memastikan informasi yang diterima tidak diubah dari aslinya.

(3) Otentikasi, untuk memastikan realibilitas asal informasi.

(4) *Availability*, yang menjamin pengguna untuk dapat mengakses layanan WSN kapan saja dibutuhkan meskipun sedang terjadi serangan.

(5) Kebaruan data dan kunci, dimana data yang dihasilkan dan kunci yang dipakai adalah yang terbaru.

(6) Pengaturan mandiri dimana simpul sensor bebas dan fleksible untuk secara mandiri bereaksi terhadap situasi bermasalah.

(7) Otorisasi, dimana hanya entitas yang berwenang saja yang bisa mengakses layanan dan sumber daya jaringan.

(8) *Non-repudiant*, dimana suatu simpul tidak dapat mengingkari telah mengirim pesan yang telah dikirim sebelumnya.

(9) Sinkronisasi waktu untuk sebagian besar aplikasi dalam WSN.

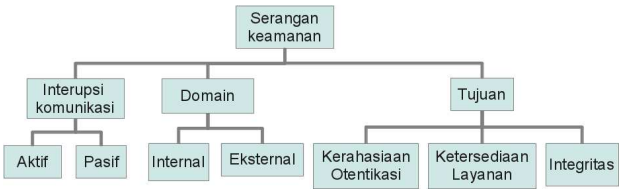
(10) *Secure localization*, terutama untuk sensor yang membutuhkan informasi lokasi secara akurat dan otomatis.

(11) *Forward/backward secrecy* dimana suatu sensor tidak diijinkan untuk mengetahui informasi setelah sensor tersebut meninggalkan jaringan dan sensor yang baru bergabung tidak dapat mengetahui pesan yang dikirimkan sebelumnya.

2.2 Serangan Keamanan

Terdapat beberapa jenis serangan keamanan terhadap WSN sebagaimana terlihat dalam Gambar

2. Berdasarkan jenis interupsi pada komunikasi jaringan sensor, serangan dapat dibagi menjadi 2 yaitu serangan pasif dan aktif [12][13]. Pada serangan pasif, pihak tidak berwenang dapat mengakses paket data tanpa melakukan interupsi terhadap komunikasi jaringan misalnya dengan penyadapan dan analisis trafik. Sedangkan serangan aktif mengganggu fungsionalitas jaringan dengan melancarkan serangan *denial of service* (DoS) seperti jamming dan penyedotan daya sensor.



Gambar 2. Jenis serangan keamanan

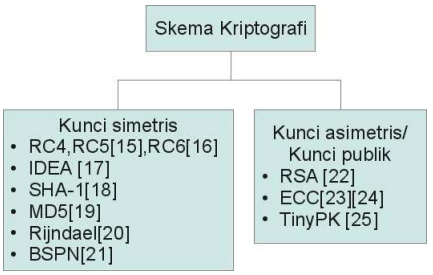
Asal serangan dapat diklasifikasikan menjadi 2 yaitu serangan eksternal dan internal [14]. Serangan eksternal berasal dari simpul yang bukan merupakan bagian dari jaringan sensor. Sedangkan serangan internal dapat berasal dari simpul yang menjadi bagian jaringan yang dikuasai penyerang, atau dari penyerang yang mengetahui sandi, kode dan data dari simpul yang sah dan melakukan penyerangan dengan peralatan sekelas laptop.

Menurut tujuannya, serangan dapat dibagi menjadi 3 jenis yaitu serangan terhadap kerahasiaan dan otentikasi, serangan terhadap ketersediaan layanan dan serangan terhadap integritas data [10]. Teknik kriptografi standar dapat mengatasi serangan terhadap kerahasiaan dan otentikasi seperti penyadapan, *packet replay*, dan *spoofing*. Serangan terhadap ketersediaan layanan sering juga disebut dengan *denial of service* (DoS) yang mana merupakan suatu kejadian yang melemahkan atau mencoba mengurangi kapasitas jaringan untuk sehingga jaringan tidak bekerja sesuai fungsi yang seharusnya [10]. Sedangkan dalam serangan terhadap integritas data, penyerang bertujuan membuat jaringan menerima data yang salah.

3. MEKANISME KEAMANAN

3.1 Kriptografi

Kriptografi adalah metode enkripsi dasar yang digunakan dalam menerapkan keamanan. Pemilihan kriptografi memegang peranan penting dalam keamanan WSN [6]. Secara umum terdapat dua pendekatan yaitu kriptografi kunci simetris dan asimetris (kunci publik) sebagaimana terlihat dalam Gambar 3 [15][16][17][18][19][20][21][22][23][24][25].
Kriptografi kunci simetris menggunakan kunci yang sama untuk proses enkripsi dan dekripsi sedang metode kunci publik (asimetris) menggunakan kunci yang berbeda untuk enkripsi dan dekripsi.



Gambar 3. Skema Kriptografi

Tabel I. Perbandingan konsumsi energi kunci publik (dalam mJ)

Algoritma	Pjg Kunci (bit)	*Signature*		Pertukaran Kunci	
		sign	*verify*	klien	server
RSA	1024	304	11,9	15,4	304
	2048	2302,7	53,7	57,2	2302,7
ECC	160	22,82	45,09	22,3	22,3
	244	61,54	121,98	60,4	60,4

Sumber: [15]

Tabel II. Perbandingan konsumsi waktu komputasi publik (dalam detik)

Algoritma	Pjg Kunci (bit)	*Signature*		Pertukaran Kunci	
		sign	*verify*	klien	server
RSA	1024	22,03	0,86	1,12	22,03
	2048	166,85	3,89	4,14	166,85
ECC	160	1,65	3,27	1,62	1,62
	244	4,46	8,84	4,28	4,38

Sumber: [15]

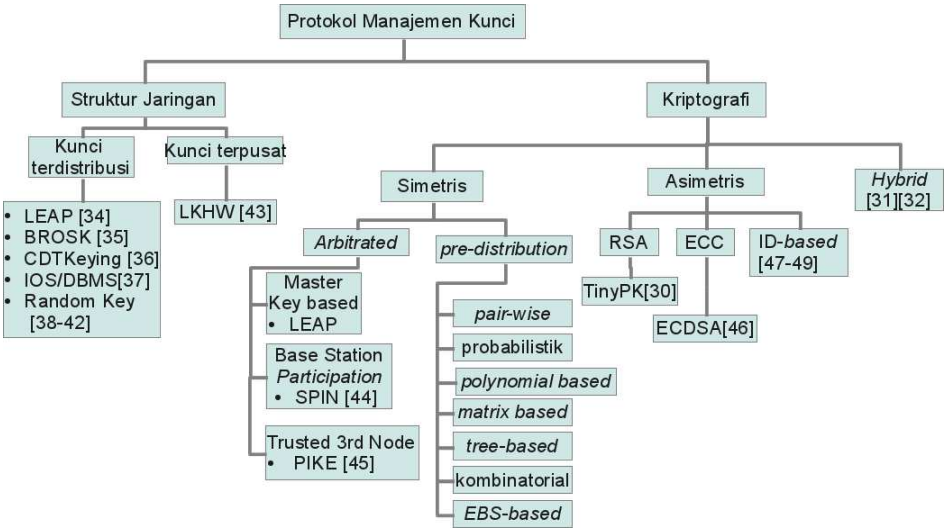
Perbandingan konsumsi energi untuk kunci publik disajikan dalam [26] sebagaimana terlihat dalam Tabel I dan perbandingan waktu komputasi terkait dalam Tabel II [27]. Dalam hasil tersebut diperlihatkan bahwa ECC menawarkan keamanan yang sebanding dengan RSA dengan kunci yang lebih kecil sehingga mengurangi komputasi. Sebagai contoh, RSA dengan kunci 1024 (RSA-1024) bit menyediakan tingkat keamanan yang bisa diterima pada kebanyakan aplikasi pada saat ini, setara dengan ECC dengan kunci 160 bit.

Pengujian terhadap algoritma kunci simetris ditunjukkan dalam Tabel III [28]. Dari tabel tersebut terlihat bahwa secara umum, kriptografi kunci simetris jauh lebih unggul dari kriptografi kunci publik dalam hal kecepatan dan kebutuhan energi. Dalam hal ini, skema kriptografi kunci publik kurang

Tabel III. Perbandingan performa algoritma kunci simetris dalam WSN dalam satuan μs

Algoritma	Ukuran	Aksi	Atmega 103	Atmega 128	M16C/10	StrongARM	Xscale (400)	Xscale (200)	Sparc (440)
MD5	0	Digest	5863	1466	1083	46	26	53	23
	1-26	Digest	5890	1473	1075	46	26	53	23
	62-80	Digest	10888	2722	2011	74	45	90	39
SHA-1	1	Digest	15249	3812	2651	69	12	102	27
	3	Digest	15781	3945	5303	69	12,3	103	27
	56	Digest	14543	3636	7955	133	25,8	205	55
	64	Digest	31107	7777	10907	145	25,7	207	56
RC5	16	Init	9641	2410	2074	41	45	91	28
		Enkripsi	1651	413	197	3	3	6	2
		Dekripsi	1636	409	202	3	3	7	2
IDEA	16	Init Enk	1523	381	727	26	15,54	47	11
		Init Dek	9417	2354	1927	76	25,16	69	36
		Enkripsi	2555	325	596	16	3,24	17	9
		Dekripsi	2614	325	597	16	3,27	17	9
RC4		Init	1886	472	2455	155	66,8	216	96
		Enkripsi	344	86	123	10	5	9	4

Sumber: [28]



Gambar 4. Protokol Manajemen Kunci

cocok diterapkan pada WSN karena keterbatasan sumber daya sensor. Meskipun beberapa penelitian seperti pada [29][30] menunjukkan kemungkinan untuk menerapkan kriptografi kunci publik pada WSN dengan memilih algoritma yang tepat, tetapi penggunaan kunci privat pada kriptografi asimetris tetap sulit diterapkan karena masalah komputasi dan kebutuhan energi. Akan tetapi, penggunaan kriptografi kunci simetris membutuhkan manajemen kunci yang efisien dan fleksibel. Beberapa riset mencoba menggabungkan 2 skema ini secara bersamaan [31][32]. Untuk otentikasi digunakan skema kunci publik berbasis ECC dan dilakukan pada *base station* serta untuk operasi yag terkait dengan kerahasiaan dan integritas data digunakan kunci simetris pada sensor.

3.2 Manajemen Kunci

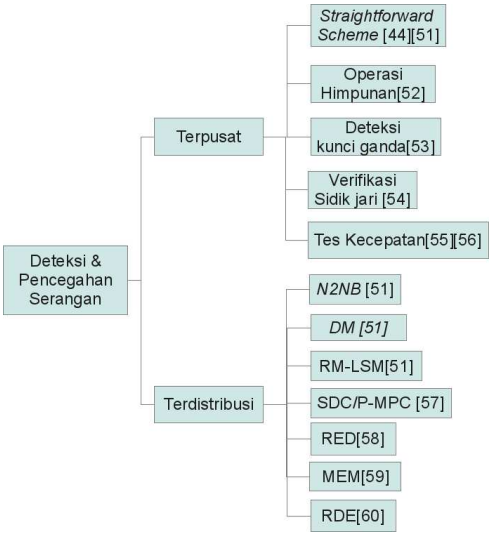
Manajemen kunci digunakan untuk menentukan kunci yang digunakan antar simpul dengan cara aman dan terpercaya. Skema yang digunakan harus mampu mendukung penambahan dan pengurangan simpul secara dinamis dan karena keterbatasan sumber daya, protokol managemen kunci ini harus ringan. Taksonomi manajemen kunci diulas dalam [2][6][33] yang diringkas sebagaimana terlihat pada Gambar 4 [30][31][32][34][35][36] [37][38][39][40][41][42][43][44][45][46][47][48] [49].

Berdasar struktur jaringan terdapat 2 tipe manajemen kunci yaitu kunci terpusat dan terdistribusi [6]. Dalam skema kunci terpusat, hanya ada satu entitas yang mengatur pembangkitan

dan pendistribusian kunci yang disebut dengan *Key Distribution Center* (KDC). Meskipun skema ini dapat mengurangi kebutuhan penyimpanan pada simpul sensor tetapi berdampak pada tinggi biaya komunikasi dan kerentanan kegagalan terpusat pada satu titik saja. Sedangkan pada protokol terdistribusi, digunakan beberapa controller berbeda untuk mengatur kunci, yang memungkinkan kerentanan kegagalan tidak berada pada satu titik dan memiliki skalabilitas yang lebih baik.

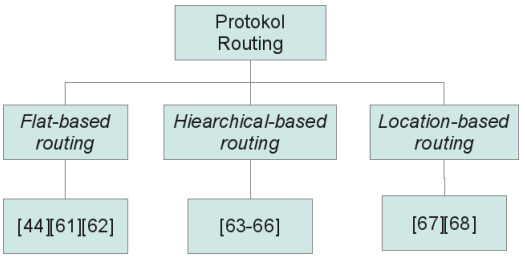
Klasifikasi lain berdasarkan kriptografi yang digunakan: simetris, asimetris dan campuran [2]. Skema kriptografi simetris terbagi menjadi skema berbasis entitas (*arbitrated*) dimana pembentukan dan pendistribusian kunci berdasar pada entitas yang dipercaya, dan skema pre-distribusi, dimana simpul sensor menyimpan beberapa kunci awal sebelum disebarkan. Setelah disebarkan, sensor menggunakan kunci awal tersebut untuk mengatur komunikasi yang aman. Dalam skema kriptografi asimetris, algoritma kunci publik RSA dan ECC merupakan skema yang banyak digunakan, disamping skema berdasar identitas (ID).

3.3 Deteksi dan Pencegahan Serangan



Gambar 5. Mekanisme deteksi dan pencegahan serangan

Untuk meningkatkan keamanan sistem, diperlukan mekanisme deteksi serangan meskipun pada sebagian besar skema keamanan mampu membatasi efek serangan pada sistem. Secara umum, deteksi serangan dibagi 2 pendekatan yaitu pendekatan terpusat dan pendekatan terdistribusi atau *neighbour's cooperative* [6]. Pada pendekatan pertama, stasiun pusat digunakan untuk mendeteksi serangan. Kelemahannya adalah peningkatan trafik *routing* dari simpul tertentu ke stasiun pusat.



Gambar 6. Protokol Routing

Sedangkan pendekatan kedua memanfaatkan simpul yang berdekatan untuk mengumpulkan informasi tentang simpul tetangganya dan membuat keputusan kolektif untuk mendeteksi serangan. Hal ini akan meningkatkan proses komputasi dan tugas pengawasan simpul yang berdekatan. Taksonomi mekanisme deteksi dan pencegahan serangan ini terlihat pada Gambar 5 [50][44][51][52][53][54][55][56][57][58][59][60].

3.4 Routing

Terdapat beberapa jenis serangan yang melumpuhkan *routing* seperti Sybil, wormhole, sinkhole, HELLO flood [61]. Hal ini terjadi karena banyak protokol *routing* WSN yang terlalu sederhana dengan fitur keamanan yang sedikit. Sedangkan adaptasi protokol *routing* dari jaringan *ad-hoc* masih memerlukan penelitian lebih lanjut. Berdasarkan struktur jaringan, protokol *routing* diklasifikasikan menjadi 3, *flat-based*, *hierarchical-based* dan *location-based routing* [62]. Dalam *flat-based routing*, semua simpul mempunyai peran dan fungsi yang sejajar, berlawanan dengan simpul dalam *hierarchical-based routing*, dimana simpul memiliki fungsi yang berbeda dalam jaringan. Sedangkan pada *location-based routing*, posisi lokasi simpul digunakan untuk melewatkan data di jaringan. Gambaran klasifikasi skema *routing* WSN seperti terlihat pada Gambar 6 [61][44][62][63][64][65][66][67][68].

4. KESIMPULAN

WSN mempunyai prospek yang menjanjikan dalam banyak aplikasi. Dengan karakteristik yang unik dan keterbatasannya, diperlukan pendekatan keamanan yang berbeda dengan jaringan biasa. Dalam makalah ini dibahas berbagai aspek yang terkait dengan keamanan WSN seperti karakteristik WSN, persyaratan keamanan, jenis serangan dan pertahanannya serta mekanisme keamanan yang ada pada WSN.

Berdasarkan studi literatur yang telah dilakukan, untuk memenuhi layanan keamanan informasi pada WSN, disarankan beberapa hal berikut:

(1) Menggunakan kriptografi kunci simetris sebagai dasar layanan keamanan dengan pertimbangan biaya komputasi dan energi yang dibutuhkan.
(2) Menggunakan manajemen kunci terdistribusi untuk mengurangi kerentanan kegagalan, yang dikombinasikan dengan skema kunci pre-distribusi.
(3) Menggunakan sistem deteksi serangan terpusat dengan pertimbangan tidak memberatkan proses komputasi pada setiap simpul.

Daftar Pustaka

[1] H. Yang, F. Y. Y. Yuan, S. Lu, W. Arbaugh, and L. Angeles, "Toward resilient security in wireless sensor networks," in *MobiHoc 05*, 2005, pp. 34–45.

[2] J. Zhang and V. Varadharajan, "Wireless sensor network key management survey and taxonomy," *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 63–75, 2010.

[3] H. Chan and A. Perrig, "Security and privacy in sensor networks," *Computer*, vol. 36, no. 10, pp. 103–105, 2003.

[4] P. Mohanty, S. Panigrahi, N. Sarma, and S. S. Satapathy, "Security issues in wireless sensor network data gathering protocols: a survey," *Journal of Theoritical and Applied Information Technology*, vol. 13, no. 1, pp. 14–27, 2010.

[5] T. Zia and A. Zomaya, "Security issues in wireless sensor networks," in *ICSNC 2006*, 2006, p. 40.

[6] X. Chen, K. Makki, and K. Yen, "Sensor network security: A survey," *IEEE Communications Survey & Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[7] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[8] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, *Security in Distributed, Grid, Mobile and Pervasive Computing*. CRC Press, 2007, ch. Wireless Sensor Network Security: A Survey.

[9] Z. Bojkovic, B. Bakmaz, and M. Bakmaz, "Security issues in wireless sensor networks," *International Journal of Communication*, vol. 2, no. 1, 2008.

[10] J. Sen, "A survey on wireless sensor network security," *International Journal of Communication Network and Information Security*, vol. 1, no. 2, pp. 59–82, 2009.

[11] Y. Zhang, X. Li, L. He, X. Ma, and L. Zeng, "A dynamic security protocol for the heterogeneous rfid and wireless sensor network," *Energy Procedia*, vol. 13, pp. 337–346, 2011.

[12] V. Manju, "Study of security issues in wireless sensor network," *International Journal of Engineering Science*, vol. 3, no. 10, pp. 7347–52, 2011.

[13] K. Stewart, T. Haniotakis, and S. Tragoudas, "Securing sensor networks: A novel approach that combines encoding, uncorrelation and node disjoint transmission," *Ad Hoc Networks*, vol. 10, no. 3, pp. 328–38, 2012.

[14] H. Chen, W. Lou, and Z. Wang, "A novel secure localization approach in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, 2010.

[15] R. Rivest, "The rc5 encryption algorithm," *Fast Software Encryption*, pp. 86–96, 1995.

[16] R. Rivest, M. Robshaw, R. Sidney, and Y. Yin, "The rc6 block cipher," in *The First Advanced Encryption Standard Conference*, 1998, p. 16.

[17] X. L. adn J.L. Massey, "A proposal for a new block encryption standard," in *EUROCRYPT '90*. Springer-Verlag, 1991, pp. 389–404.

[18] D. Eastlake and P. Jones, "Us secure hash algorithm 1(sha1)," RFC 3174, September 2001.

[19] R. Rivest, "The md5 message-digest algorithm," RFC 1321, April.

[20] J. Daemen and V. Rijmen, "Aes proposal: Rijndael," in *Proceedings of 1st AES Conference*, 1998.

[21] L. Si, Z. Ji, and Z. Wang, "The application of symmetric key cryptographic algorithms in wireless sensor networks," *Physics Procedia*, vol. 25, pp. 552–59, Jan 2012.

[22] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 26, no. 1, pp. 96–99, 1983.

[23] V. Miller, "Use of elliptic curves in cryptography," in *Lecture Notes in Computer Sciences: 218 on Advances in Cryptology- CRYPTO 85*. Springer-Verlag, 1986, pp. 417–26.

[24] N. Kobiltz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, pp. 203–09, 1987.

[25] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "Tinypk: Securing sensor networks with public key technology," in *Proc. of 2nd ACM workshop on Security of Ad Hoc and Sensor Networks '04*, 2004, pp. 59–64.

[26] A. S. Wander, N. Gura, H. Eberle, V. Gupta, S. C. Shantz, and S. Cruz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proceedings of 3rd IEEE International Conference on Pervasive Computing and Communications*, 2005, pp. 324–28.

[27] F. Amin, A. Jahangir, and H. Rasifard, "Analysis of public-key cryptography for wireless sensor networks security," in *Proceedings of World Academy of Science, Engineering and Technology*, vol. 31, July 2008, pp. 530–535.

[28] S. U. Rehman, M. Bilal, B. Ahmad, K. M. Yahya, A. Ullah, and O. U. Rehman, "Comparison based analysis of different cryptographic and encryption techniques using message authentication code (mac) in wireless sensor networks (wsn)," *International Journal of Computer Science Issues*, vol. 9, no. 1, 2012.

[29] S. Jin and H. Yu-pu, "The collaborative design broadcast encryption on heterogeneous sensor," *Energy Procedia*, vol. 13, pp. 809–14, 2011.

[30] T. Yan and Q. Wen, "A security improved protocol for wireless sensor networks based on public key sertificate," *Energy Procedia*, vol. 13, pp. 708–13, 2011.

[31] J. Zhang and V. Varadharajan, "Group-based wireless sensor network security scheme," in *The 4th International Conference on Wireless and Mobile Communications (ICWMC 2008)*, July 2008.

[32] D. Huang, M. Mehta, D. Medhi, and L. Harn, "Location-aware key management scheme for wireless sensor networks," in *Proceedings of ACM Workshop on Security of Ad hoc and Sensor Networks (SASN04)*, 2004, pp. 29–42.

[33] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor network," *IEEE Comm. Surveys & Tutorials*, vol. 8, no. 2, pp. 2–23, 2006.

[34] S. Zhu, S. Setia, and S. Jajodia, "Leap: Efficient security mechanism for large scale distributed sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, 2003, pp. 62–72.

[35] d. I. V. B. Lai, S. Kim, "Scalable session key construction protocols for wireless sensor networks," IEEE Workshop on Large Scale Real Time and Embedded Systems, 2002.

[36] S. Cametepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," in *Proceedings of the 9th European Symposium on Research Computer Security*, 2004.

[37] J. Lee and D. Stinson, "Deterministic key pre-distribution schemes for distributed sensor networks," in *Proceedings of Selected Areas in Cryptography*, 2004, pp. 294–307.

[38] W. Du, J. Deng, Y. Han, and P. Varshney, "A pair-wise key pre-distribution scheme for wireless sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, 2003, pp. 42–51.

[39] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2003, p. 197.

[40] J. Lee and D. Stinson, "A combinatorial approach to key pre-distribution for distributed sensor networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference*, 2005.

[41] W.-S. Li, C.-W. Tsai, M. Chen, W.-S. Hsieh, and C.-S. Yang, "Threshold behavior of multi-path random key pre-distribution for sparse wireless sensor network," *Mathematical and Computer Modelling*, 2012.

[42] C. Chen and C. Li, "Dynamic session-key generation for wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, no. 1, 2008.

[43] R. D. Pietro, L. Mancini, Y. Law, S. Etalle, and P. Havinga, "Lkhw: A directed diffusion-based secure multi- cast scheme for wireless sensor networks," in *Proceedings of the 32nd ICPPW 03*, 2003, pp. 397–406.

[44] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "Spins: Security protocols for sensor networks," *Wireless Networks*, vol. 8, no. 5, pp. 521–34, 2002.

[45] H. Chan and A. Perrig, "Pike: Peer intermediaries for key establishment in sensor networks," *IEEE INFOCOM*, pp. 524–35, 2005.

[46] D. Hankerson, A.Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. Springer-Verlag, 2004.

[47] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *Advance in Cryptology-crypto, Lecture Notes in Computer Science*, vol. 2139, pp. 213–19, 2001.

[48] G. Yang, C. Rong, C.Veigner, J. Wang, and H. Cheng, "Identity-based key agreement and encryption for wireless sensor networks," *International Journal of Computer Science and Network Security*, vol. 6(5B), pp. 182–89, 2006.

[49] Z. Feng, W. Wu, and H. Nansong, "Identity-based key agreement protocols in wireless sensor networks," *Energy Procedia*, vol. 13, pp. 5676–80, 2011.

[50] W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting node replication attacks in wireless sensor networks: A survey," *Journal of Network and Computer Applications*, vol. 35, no. 3, pp. 1022–34, 2012.

[51] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proceedings of the 26th IEEE Symposium on Security and Privacy (S&P 05)*, 2005, pp. 49–63.

[52] H. Choi, S. Zhu, and T. F. L. Porta, "Set: Detecting node clones in sensor networks," in *Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007*, 2007, pp. 341–350.

[53] R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. Kandemir, "On the ddetection of clones in sensor networks using random key predistribution," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 37, p. 124658, 2007.

[54] K. Xing, F. Liu, X. Cheng, and D. H. C. Du, "Real-time detection of clone attacks in wireless sensor networks," in *The 28th International Conference on Distributed Computing Systems*, 2008, pp. 3–10.

[55] J.-W. Ho, M. Wright, and S. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in *Proceedings of the 28th IEEE Conference on Computer Communications (INFOCOM 09)*, 2009, p. 177381.

[56] S. K. Das and J. won Ho, "A synopsis on node compromise detection in wireless sensor networks using sequential analysis," *Computer Communications*, vol. 34, no. 17, pp. 2003–2012, 2012.

[57] B. Zhu, S. Setia, V. Gopala, K. Addada, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in *The 23rd Annual Computer Security Application Conference*, 2007, pp. 257–67.

[58] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in *Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, 2007, p. 80.

[59] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in *Proceedings of the 17th IEEE International Conference on Network Protocols*, 2009, pp. 284–93.

[60] Z. Li and G. Gong, "Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks," in *Proceedings of the 6th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, 2009, p. 10305.

[61] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 23, pp. 293–315, 2003.

[62] J. N. Al-Karaki and A. E. Kamal, "Routing technique in wireless sensor networks: A survey," *IEEE Wireless Communication*, vol. 11, no. 6, pp. 6–28, 2004.

[63] C. Hong-bing, Y. Geng, and H. U. Su-jun, "Nhrpa: a novel hierarchical routing protocol algorithm for wireless sensor networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 15, pp. 75–81, 2008.

[64] M. Zeynali, A. Mollanejad, and L. M. Khanli, "Novel hierarchical routing protocol in wireless sensor network," *Procedia Computer Science*, vol. 3, pp. 292–300, Jan 2011.

[65] D. Liu and P. Ning, "Multi-level tesla: Broadcast authentication for distributed sensor networks," in *Proceedings of the 10th Annual Network and Distributed Systems Security Symposium*, vol. V, 2003, p. 263276.

[66] M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "Minisec: A secure sensor network communication architecture," in *Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN 07)*, 2007, p. 479488.

[67] H. C. Leligou, T. Zahariadis, F. Alvarez, and P. Karkazis, "Secure geographic routing in ad hoc and wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, p. Article ID 975607, 2010.

[68] J. Deng, R. Han, and S. Mishra, "Insens: Intrusion-tolerant routing for wireless sensor networks," *Computer Communications*, vol. 29, no. 2, pp. 216–230, Jan 2006.