DIAGRAM SITASI PAPER

KEAMANAN JARINGAN SENSOR NIRKABEL: SERANGAN DAN SOLUSINYA

Disusun Oleh:

Andre Herviant Juliano

09011181520025

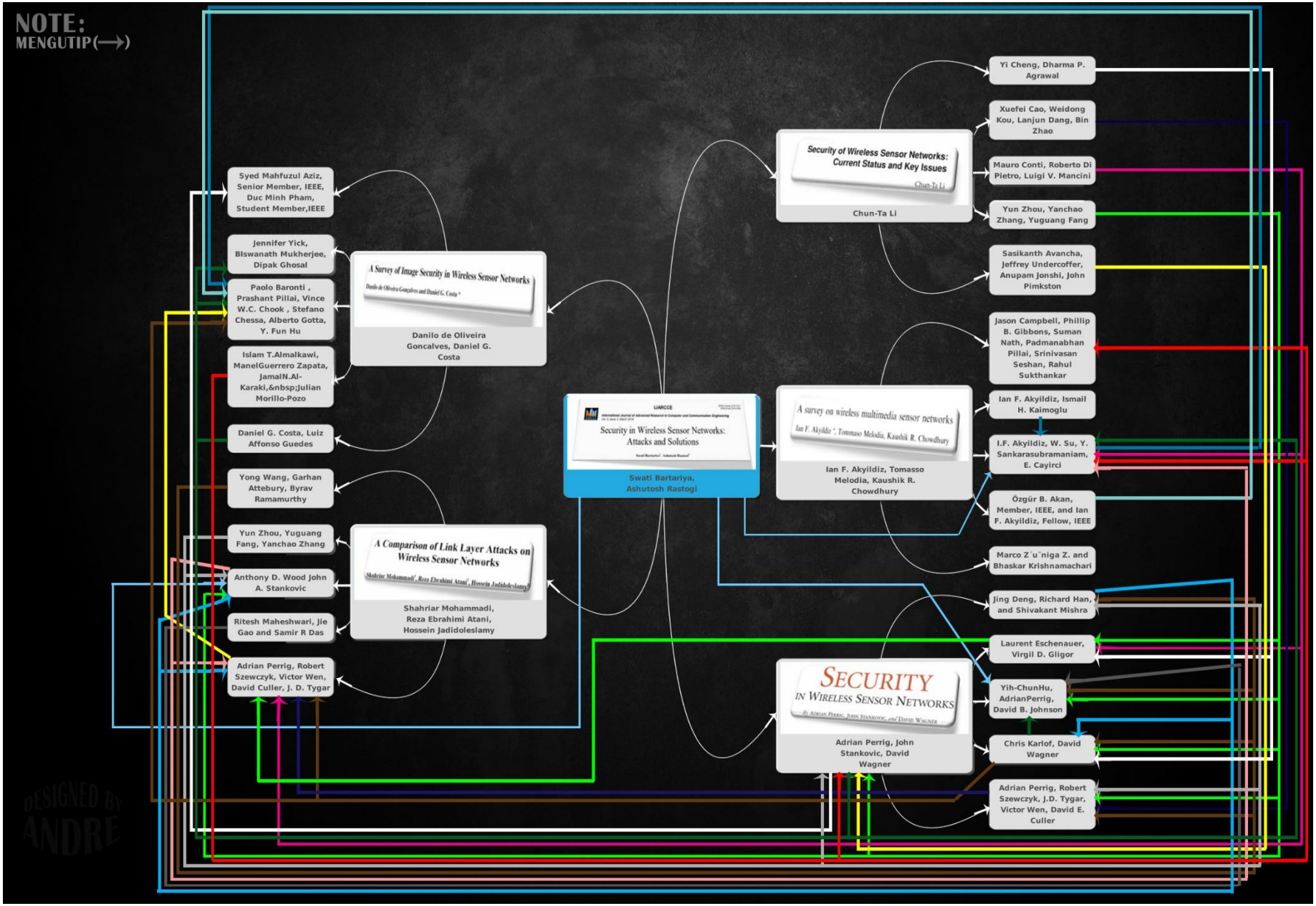
SK2A

PROGRAM STUDI SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2016


NOTE:
MENGUTIP(⟶)
Syed Mahfuzul Aziz, Senior Member, IEEE, Duc Minh Pham, Student Member,IEEE
Jennifer Yick, BIswanath Mukherjee, Dipak Ghosal
Paolo Baronti , Prashant Pillai, Vince W.C. Chook , Stefano Chessa, Alberto Gotta, Y. Fun Hu
Islam T.Almalkawi, ManelGuerrero Zapata, JamalN.Al-Karaki, Julian Morillo-Pozo
Daniel G. Costa, Luiz Affonso Guedes
Yong Wang, Garhan Attebury, Byrav Ramamurthy
Yun Zhou, Yuguang Fang, Yanchao Zhang
Anthony D. Wood John A. Stankovic
Ritesh Maheshwari, Jie Gao and Samir R Das
Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar
A Survey of Image Security in Wireless Sensor Networks
Danilo de Oliveira Goncalves, Daniel G. Costa
A Comparison of Link Layer Attacks on Wireless Sensor Networks
Shahriar Mohammadi, Reza Ebrahimi Atani, Hossein Jadidoleslamy
Security in Wireless Sensor Networks: Attacks and Solutions
Swati Bartariya, Ashutosh Rastogi
Security of Wireless Sensor Networks: Current Status and Key Issues
Chun-Ta Li
A survey on wireless multimedia sensor networks
Ian F. Akyildiz, Tomasso Melodia, Kaushik R. Chowdhury
SECURITY IN WIRELESS SENSOR NETWORKS
Adrian Perrig, John Stankovic, David Wagner
Yi Cheng, Dharma P. Agrawal
Xuefei Cao, Weidong Kou, Lanjun Dang, Bin Zhao
Mauro Conti, Roberto Di Pietro, Luigi V. Mancini
Yun Zhou, Yanchao Zhang, Yuguang Fang
Sasikanth Avancha, Jeffrey Undercoffer, Anupam Jonshi, John Pimkston
Jason Campbell, Phillip B. Gibbons, Suman Nath, Padmanabhan Pillai, Srinivasan Seshan, Rahul Sukthankar
Ian F. Akyildiz, Ismail H. Kaimoglu
I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci
Özgür B. Akan, Member, IEEE, and Ian F. Akyildiz, Fellow, IEEE
Marco Z´u¨niga Z. and Bhaskar Krishnamachari
Jing Deng, Richard Han, and Shivakant Mishra
Laurent Eschenauer, Virgil D. Gligor
Yih-ChunHu, AdrianPerrig, David B. Johnson
Chris Karlof, David Wagner
Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen, David E. Culler
DESIGNED BY ANDRE

Keamanan Jaringan Sensor Nirkabel: Serangan dan Solusinya

[1] Banyak masalah yang bermunculan, jaringan sensor nirkabel menjadi solusi yang tepat. Namun, teknologi baru tanpa keamanan ini telah terbukti berbahaya. WSN atau jaringan sensor nirkabel ini sangat mencuri perhatian para peneliti karena berbagai aplikasinya . Dalam paper ini, kami mengidentifikasi ancaman dan serangan keamanan di WSN. Meskipun banyak upaya telah dilakukan pada kriptografi manajemen kunci dan pertahanan terhadap serangan DoS, namun masih banyak yang perlu diperbaiki. Mekanisme kriptografi saat mempertahankan dan mendeteksi node yang mencurigakan belum begitu sempuran, karena masih ada beberapa kegiatan mencurigakan yang tidak dapat dideteksi segera. Ada 5 (lima) jenis jaringan sensor nirkabel, antara lain *Terrestrial WSNs, Underground WSNs, Underwater WSNs, Multimedia WSNs, dan Mobile WSNs*. Kami membahas solusi kemanan dan juga menyediakan diskusi singkat untuk penelitian selanjutnya di bidang WSN. Kami telah menjelaskan aspek-aspek keamanan di WSN, antara lain: kendala keamanan, serangan dan ancaman, serta solusi keamanan. Tujuan kami adalah untuk memberikan gambaran umum tentang pendekatan keamanan WSN yang ada. Banyak persoalan yang akan terbuka dan kami ingin melihat kegiatan penelitian lebih lanjut tentang topik ini.

[2] Karena kemajuan yang signifikan dalam teknik komunikasi nirkabel dan mobile serta pengembangan yang luas dari aplikasi potensial, Wireless Sensor Networks (WSNs) atau jaringan sensor nirkabel telah menarik perhatian yang besar dalam beberapa tahun terakhir. WSNs terbentuk secara dinamis oleh sejumlah node sensor dan node manager dengan daya yang tahan lama. Jaringan sensor nirkabel mengatur sendiri sistemnya, sistem itu terdiri dari sensor umum, node manajer dan *back-end* data pusat. Jaringan sensor nirkabel telah banyak digunakan dalam aplikasi praktis, seperti pemantauan kebakaran hutan, deteksi tujuan militer, bidang medis atau ilmu pengetahuan dan bahkan dalam kehidupan rumah kami. Namun, WSNs sangat mudah di deteksi oleh penyerang karena komunikasi nirkabel menggunakan media transmisi siaran. Oleh karena itu, penyerang bisa mengetahui semua lalu-lintas jaringan, menyuntikkan paket berbahaya, memutar ulang pesan lama, atau membahayakan node sensor. Umumnya, node sensor sangat kesusahan pada dua masalah keamanan,antara lain melindungi privasi dan otentikasi node.

Kami berpendapat bahwa tidak ada skema keamanan tunggal yang sangat ideal untuk semua aplikasi, di mana jaringan sensor yang digunakan dan teknik kriptografi yang diadopsi harus sesuai dengan penerapan arsitektur yang telah ditentukan dan persyaratan keamanan di WSNs. Ada beberapa masalah penelitian selanjutnya yang harus dipertimbangkan untuk jaringan sensor nirkabel dalam bab ini. Ada juga faktor penentu keberhasilan dari jaringan sensor nirkabel, antara lain: *Soft message encryption, Multiple communication paths, Multiple communication paths, Malicious node detection, Node revocation-awareness.*

[3] Jaringan sensor nirkabel semakin mencuri perhatian di kalangan para peneliti. Dalam beberapa tahun terakhir, banyak pemantauan yang telah dilakukan, kontrol dan pelacakan aplikasi telah dirancang untuk skenario yang berbeda. Untuk jaringan seperti itu, sensor kamera aktif dapat mengambil data visual dari pemantauan lapangan, memberikan informasi yang penting untuk banyak aplikasi. Secara umum, jaringan memiliki keterbatasan sumber daya pemrosesan, memori, energi dan bandwidth transmisi, dan memaksakan banyak masalah desain. Namun demikian, sekelompok aplikasi juga mungkin memiliki persyaratan keamanan, yang membawa tambahan rumit untuk ditangani. Kebanyakan mekanisme keamanan tradisional digunakan untuk jaringan populer seperti Internet, tidak cocok untuk jaringan sensor nirkabel, karena menuntut penyelidikan yang tepat di bidang ini. Dalam paper ini, kami meninjau perkembangan terakhir pada enkripsi dan privasi dalam penyebaran jaringan sensor nirkabel digunakan untuk transmisi dari gambar, meninjau pendekatan inovatif untuk memberikan berbagai tingkat keamanan. Mekanisme keamanan bisa dikatakan penting dalam desain WSN. Karya terakhir telah fokus pada mekanisme inovatif untuk memberikan berbagai tingkat keamanan tergantung pada sumber daya yang tersedia dari jaringan sensor. Dalam konteks ini, enkripsi sangat penting untuk aplikasi WSN, karena jaringan ini sangat rentan terhadap kegagalan keamanan dengan sifat nirkabel. Enkripsi selektif gambar merupakan mekanisme penting untuk menjamin keamanan dalam jaringan dengan keterbatasan sumber daya. Mekanisme enkripsi tradisional tidak mungkin untuk WISN karena melebihi batas dari komputasi dan komunikasi, solusi yang mungkin tepat adalah dengan mengkombinasikan pengkodean algoritma dengan kriptografi. Otentikasi yang dilakukan dengan cara watermarking dan memantau keamanan citra , serta masalah-masalah relevan yang disurvei dalam pekerjaan ini. Tinjauan yang dilakukan telah membawa kontribusi yang signifikan untuk penyelidikan dalam jaringan sensor gambar nirkabel dan berpotensi untuk mendukung penelitian selanjutnya.

[4] Kendala yang berat dan menuntut lingkungan jaringan sensor nirkabel untuk membuat keamanan komputer dalam sistem ini lebih menarik daripada jaringan konvensional. Namun, beberapa sifat dari jaringan sensor dapat membantu mengatasi masalah untuk membangun kemanan jaringan. Pertama, kita memiliki kesempatan untuk membuat solusi keamanan ke dalam sistem ini dari awal, karena masih dalam desain dan tahap penelitian. Kedua, banyak aplikasi yang mungkin melibatkan penyebaran jaringan sensor di dalam domain administrasi tunggal, serta menyederhanakan model ancaman. Ketiga, dimungkinkan untuk mengeksploitasi redundansi, skala, dan karakteristik fisik lingkungan. Jika kita membangun jaringan sensor sehingga mereka terus beroperasi bahkan jika beberapa fraksi sensor mereka terganggu, kami akan menggunakan sensor yang lebih kuat untuk menahan serangan lebih lanjut. Pada akhirnya, aspek unik dari jaringan sensor memungkinkan pertahanan baru yang tidak tersedia di jaringan konvensional. Banyak masalah lain juga, sehingga perlu penelitian lebih lanjut. Salah satunya adalah bagaimana mengamankan link komunikasi nirkabel dalam menghadapi *eavesdropping*, mengubah sesuatu secara ilegal, analisis lalu lintas, dan penolakan layanan. Lainnya melibatkan keterbatasan sumber daya. Arah yang berkelanjutan termasuk protokol asimetris di mana sebagian besar beban komputasi jatuh pada base station dan kriptografi yang efisien pada perangkat low-end. Akhirnya, menemukan cara untuk mentolerir kurangnya keamanan fisik, mungkin melalui redundansi atau pengetahuan tentang lingkungan fisik, akan tetap menjadi tantangan keseluruhan yang bersifat kontinu.

[5] Dalam paper ini, kami menganalisis dimensi yang berbeda dari keamanan WSN, menyajikan berbagai macam serangan lapisan link WSNs dan mengklasifikasikannya; kami mengklasifikasikan dan membandingkan serangan link layer WSNs berdasarkan perbedaan fitur yang diekstraksi dari link layer WSN ini, yaitu sifat serangan, seperti model ancaman WSNs, serangan link layer, tujuan dan hasil, strategi dan efek, serta teknik pertahanan dalam menangani serangan.

[6] Kami membahas penelitian tentang *Wireless Multimedia Sensor Networs (WMSNs)*, dan garis besar dari tantangan penelitian utama. Algoritma, protokol, dan perangkat keras untuk pengembangan WMSNs, serta membahas masalah-masalah penelitian secara terperinci. Kemudian membahas solusi yang ada dan membuka masalah penelitian di *Application, transport, network, link, dan physical layer* dari banyak komunikasi, bersamaan dengan kemungkinan sinergi dan optimasi cross-layer. Kami menunjukkan bagaimana karya terbaru yang dilakukan di *Wyner Ziv Coding* pada *application layer*, khusus untuk *transport layer*,

kelambatan pembatasan routing, multi-channel protokol MAC, dan teknologi UWB. Kami percaya bahwa bidang penelitian ini akan menarik perhatian banyak peneliti dan akan mendorong kemampuan kita untuk mengamati lingkungan fisik dan berinteraksi dengannya.

Daftar Pustaka

[1] Bartariya, S., & Rastogi, A. (2016). Security in Wireless Sensor Networks : Attacks and Solutions, *5*(3), 214–220. http://doi.org/10.17148/IJARCCE.2016.5352.

[2] Chun-Ta Li," Security of Wireless Sensor Networks: Current Status and Key Issues".

[3] Danilo de Oliveira Gonçalves and D.G. Costa, "A Survey of Image Security in Wireless Sensor Networks", J. Imaging 2015, 1.

[4] A .Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks", Communications of the ACM, June 2004/Vol. 47, No. 6.

[5] S. Mohammadi, R.E. Atani, H. Jadidoleslamy," A Comparison of Link Layer Attacks on Wireless Sensor Networks", Journal of Information Security, 2011, 2, 69-84.

[6] I.F. Akyildiz, T. Melodia, K.R. Chowdhury,"A survey on wireless multimedia sensor networks", Computer Networks 51 (2007) 921–960.