2007

Wireless and Sensor Networks Security (WSNS): A Retrospection

Falko Dressler
University of Erlangen

Yong Guan
Iowa State University

Zhen Jiang
West Chester University of Pennsylvania, zjiang@wcupa.edu

Recommended Citation
Dressler, F., Guan, Y., & Jiang, Z. (2007). Wireless and Sensor Networks Security (WSNS): A Retrospection. *MASS 2007, IEEE International Conference on Mobile Ad hoc and Sensor Systems, 2007*, 1-6. http://dx.doi.org/10.1109/MOBHOC.2007.4428768

Wireless and Sensor Networks Security (WSNS) A Retrospection

Falko Dressler
Autonomic Networking Group
Dept. of Computer Science 7
Univ. of Erlangen, Germany
dressler@ieee.org

Yong Guan
Dept. of Electrical and Computer Engineering
Iowa State Univ., USA
yguan@iastate.edu

Zhen Jiang
Department of Computer Science
Information Assurance Center
West Chester Univ., USA
zjiang@wcupa.edu

Abstract

After three years of organizing the wireless and sensor network security (WSNS) workshop, it is time for some retrospection to the workshop objectives and the visible outcome. This review is focusing on the the quality and performance of the workshop. On the one hand, it represents a good source to recapitulate recent research topics related to security in wireless ad hoc and sensor networks. Additionally, it extrapolates future research directions that seem to be interesting and challenging for forthcoming research activities.

1. Introduction

Wireless networks have experienced an explosive growth during the last few years. Nowadays, there is a large variety of networks spanning from the well-known cellular networks to non-infrastructure wireless networks such as mobile ad hoc networks and sensor networks. Security issue is a central concern for achieving secured communication in these networks.

Beginning in 2005, a new workshop has been created focusing on security in wireless and sensor networks. The workshop was named IEEE International Workshop on Wireless and Sensor Networks Security (WSNS). Since its first year, it has been help annually in conjunction with IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS).

This one day workshop aims to bring together researchers and practitioners from wireless and sensor networking, security, cryptography, and distributed computing communities, with the goals of promoting discussions and collaborations. We are interested in novel research on all aspects of security in wireless and sensor networks and tradeoff between security and performance such as QoS, dependability, scalability, etc. In particular, the workshop primarily focuses the following topics:

- Authentication and Access Control
- Cryptographic Protocol
- Experimental Studies
- Key Management
- Information Hiding
- Intrusion Detection and Response
- Privacy and Anonymity
- Secure Localization and Synchronization
- Security and Performance Tradeoff
- Security Policy and Enforcement Issues
- Security Protocols Design, Analysis and Verification
- Secure Routing/MAC
- Surveillance and Monitoring
- Trust Management

The objective of this paper is a retrospection to the first workshops in this series. We present a short summary of the received and presented research issues. Based on this review, we outline the most challenging questions in the domain of security in wireless and sensor networks. Additionally, we provide suggestions and recommendations for further research in this area.

The rest of the paper is organized as follows. In section 2, we revisit the first WSNS workshops and provide some statistics about papers and participation. Then, in section 3, the addressed research field in the domain of security in wireless and sensor networks is summarized. Finally, section 4 concludes the paper with some recommendations for future research in the area of WSNS.

1-4244-1455-5/07/$25.00

2. WSNS - A Retrospection

The first three events of WSNS taking place in Washington DC, USA (2005), Vancouver, Canada (2006), and Pisa, Italy (2007) turned out to be extremely successful in terms of the quality of submitted papers, the participation at the conference, and the broad range of addressed topics – nevertheless still precisely focused on security in wireless networks.

Table 1 outlines the evolution of the paper submissions, accepted papers, and the according acceptance ratios (in 2005, one invited paper has been organized). The interest from the community in wireless and sensor network security is obviously growing. Fortunately, the workshop was able to keep the acceptance ratio at a level that also allows intensive discussions about ongoing work in a relaxed atmosphere.

year	submitted	accepted	ratio
2005	26+1	12	0.44
2006	24	11	0.45
2007	33	14	0.42

Table 1. Overview to acceptance ratio of WSNS over the last years.

Regarding the workshop community, it turned out that people came from all over the world. In 2006, people from nine countries presented their papers at the workshop. In 2007, people from ten countries from all over Europe, Asia, and North America got accepted their papers. The program of WSNS always included a keynote speech from some well-known researcher in the field.

Questioning the lessons learned in three years WSNS, we particularly need to mention the specific contributions of the presenting authors in varioous field fo sensor network security. In the next section, we outline these domains and review the presented papers.

3. Research Issues in Wireless and Sensor Networks Security

The objective of this section is to review the main research domains in wireless and sensor networks security that have been addressed in the past years. This review can be used in two ways. First, it provides a good summary of recently published approaches and solutions to problems related to wireless security. Thus, anyone starting research in this domain will become a broad overview to the current state of the art in this area. Secondly, the overview provides detailed references to specific research item that also show open issues to be addressed in further work.

3.1. Identified research domains

Before introducing individual contributions, we first summarize the research domains addressed by WSNS papers in the last three years. In particular, the following three domains have been addressed:

- *Key management* – Key management is still one of the most challenging issues in ad hoc networks. The question is how do multiple nodes establish shared keys and how they can revoke keys if necessary.
- *Performance and scalability* – Focusing on low resource sensor networks, the performance of secure communication protocols and cryptographic algorithms needs to be considered for protocol engineering and for developing secure applications.
- *Access control and authentication* – Access control and authentication in wireless networks is difficult as usually no complex security architectures such as IPSec or Kerberos are available.
- *Security protocols* – Agreement protocols and integrated reliability and security measures are needed in distributed low resource networks.
- *Routing and clustering* – Ad hoc routing in wireless networks requires countermeasures against two different threats. First, selfish nodes exhaust resources from the entire network without delivering any service and, secondly, routing protocols can be attacked to eavesdrop information packets.
- *Secure localization* – Localization is a major research issue in ad hoc and sensor networks. If no security measures are integrated, this essential component cannot be trusted.
- *Intrusion detection* – Attacks such as address spoofing, denial of service, and general misbehavior need to be detected early in order not to spend too much resources for transporting attack packets.

3.2. Key management

Key pre-distribution is usually preferred in mobile ad hoc networks compared to other key management solutions. The problem of this pre-distribution is the possibility that the static keys got compromised. Several solutions have been proposed to keep the impact of key disclosure small. In a key pre-distribution scheme for mobile ad hoc networks based on set systems with limited intersection sizes, the probability that a huge amount of nodes share the same pre-distributed key is minimized using set

system [20]. Differently, the asynchronous random key pre-distribution (ARPD) approach [2] is focusing on randomized schemes for efficient operation in larger networks.

Based on this idea of random key pre-distribution, state-based key management [27] additionally exploits the deployment knowledge in sensor networks, the state of sensors, in order to remove unnecessary key assignments. This approach greatly improves the performance of the key management. Focusing on sensor networks, hierarchical solutions may further improve key management. The level-based key management for in-network processing in sensor networks [13]. It uses a hierarchy to efficiently detect and to mitigate Byzantine behavior. The communication behavior in sensor networks – usually, sensors transfer the measurement data towards a base station using a tree-like structure – can also be exploited for key management. According to the hierarchies established by the communication tree, keys can be generated accordingly [6].

For group communication, often contributory group key agreement protocols are used. The applicability in mobile ad hoc networks has been investigated resulting in solution specific to ad hoc networks [21]. In a related approach, random key pre-distribution as mentioned before is extended to provide authenticated key exchange with group support for sensor networks [34].

Specific solutions for key management in ad hoc networks such as the non-interactive key agreement and progression (NIKAP) protocol [16] show the broad application range and the complex requirements on key management schemes in wireless networks.

Key management is not only about key distribution. Another important aspect is key revocation. With the gateway subset difference revocation (GSDR) [26] mechanism, a solution for efficient grouping of receivers based upon organizational characteristics while simultaneously introducing the ability to audit rekey and data transmission has been proposed.

3.3. Performance and scalability

Discussing security in wireless networks, it is evidently necessary to analyze the performance and the scalability of proposed solutions, especially if considering low-resource networks such as sensor networks. The performance of cryptographic algorithms has been evaluated on sensor nodes in order to provide precise data to be used in simulation experiments and for general protocol design in this domain [28]. Similarly, the energy consumption of security algorithms has been investigated [4]. The cost of security measures also needs to be analyzed in much larger contexts. For example, the performance of ZigBee key exchange has been investigated in 802.15.4 beacon enabled clusters [11].

Besides measurements, the design of security solutions that explicitly focus on energy efficient operation in strongly demanded for use in sensor networks. Two examples discussed at WSNS are C4W, an energy efficient public key cryptosystem for sensor networks [10] and a work on security and energy considerations for routing in hierarchical optical sensor networks [25].

3.4. Access control and authentication

With the wide acceptance of pervasive computing solutions, location-based applications and services are becoming popular. The access to such services can nevertheless still not considered secure. The most challenging issue is access control. Location-based network access control (LBAC) is a promising solution for use in WLAN environments [7].

An interesting method for peer identification in wireless networks is based on signal properties [33]. Basically, the estimated peer location and some contributing parameters are exploited for proper identification and, thus, authentication.

Similar to nodes, messages need to be authenticated. This is specifically a requirement for queries in sensor networks. n-layers query authentication in sensor networks (n-LQA) [30] ensures that, in the presence of less than n captured nodes, unauthorized queries are stopped after a small number of hops.

3.5. Security protocols

If sensor nodes cannot be hardened to persist any attack, agreement protocols can be used to explicitly tolerate a number of malicious nodes in sensor networks [1]. Application scenarios and experiences from a practical implementation of an agreement protocol have been reported.

Looking at secure communication protocols, a number of evaluations have been published that focus on various aspects of communication in wireless and sensor networks. For example, the MAC layer security in 802.15.4 networks has been deeply investigated [22]. Additionally, the sensor network encryption protocol (SNEP) has been formally analyzed [36]. From this example – a possible attack that may lead to unauthenticated access to confidential data in the network – it can be seen that formal protocol analysis is strongly required in this domain.

The unreliability of wireless communication has been continuously addressed in the wireless communications community. Specific solutions that also incorporate security measures in this investigation are for example the reliable and semi-reliable communication with authentication (RAC) algorithm [8] and the fast and efficient secure com-

munication establishing mechanisms in aero-wireless environments [12].

A system security solution in form of a middleware platform has been developed to defend against communication based attacks. It primarily focuses on the maintenance of functional module integrity in sensor networks [29].

3.6. Routing and clustering

Secure routing in ad hoc networks is essential because wireless ad hoc networks are specifically exposed to a number of threats such as attacks on the routing protocol. At WSNS, two solutions for secure routing have been proposed. First, the reputed authenticated routing for ad hoc network protocols (Reputed-ARAN) [19] represents an extension to the ARAN protocol that is well-known in the ad hoc community. Reputed-ARAN specifically addresses the problem of selfish nodes. Secondly, the trust based routing approach in ad hoc networks [24] focuses on a trust establishment scheme that exploits trust and confidence as key metrics.

Besides the development of secure routing protocols, the formal security analysis is a crucial component for secure protocol design and analysis. A flexible and mathematically rigorous formal model to analyze the security of wireless sensor network routing protocols has been proposed and tested for the security proof of a specific link-state routing protocol [3]. It has been demonstrated that formal reasoning with respect to routing security is highly beneficial.

A great number of helper function are necessary for various routing protocols. Examples include clustering techniques such as the grouping-based clustering routing protocol for wireless networks [37], topology control mechanisms for secured coverage in sensor networks [9], and secure k-connectivity properties in sensor networks [14].

3.7. Secure localization

The capability of wireless networks to exploit the communication capabilities for localization is often controversially discussed in the context of location privacy. Location based services usually fail to provide sufficient location privacy to its users. Therefore, complex solutions have been proposed based on cryptographic mechanisms to establish blind signatures. An example for a registration protocol that ensures complete protection of the users personality while providing authorization to particular services was presented at WSNS [17]. Location tracking is not only possible by relying on received wireless communication signals. Also, the principles of ad hoc routing can be exploited for location tracking attacks. The principles of using topology information for precise node localization have been discussed at WSNS [5].

On the other hand, also the localization process needs to be secured in order to prevent attacks against the network infrastructure or against location-based services. Secure localization (SeLoc) for sensor and actor networks [18] is an approach that relies on the passive reception of authentication messages. It provides means of verifying the localization procedure and to improve the localization accuracy.

Similarly, a location verification scheme using secure distance bounding protocols [32] has been proposed to prevent attacks against location-based authentication schemes.

3.8. Intrusion detection

Finally, intrusion and misbehavior detection needs to be mentioned as a key objective of security solutions in wireless and sensor networks. A good example for attack detection in such networks is the cross-layer based intrusion detection system (CIDS) for use in wireless ad hoc networks [35]. It tries to mitigate denial of service attacks that prevent authorized users from gaining access to the network. Link layer (collisions) and network layer (packet drop misdirection) measures are used in combination to detect such attacks.

An artificial immune system based approach for misbehavior detection has been investigated in order to evaluate the impact of packet injection models on the misbehavior detection performance [31]. Such solutions are of interest as they provide insight into the traffic pattern in real sensor networks.

Address spoofing is an eminent issue in wireless networks as many authentication schemes rely on correct address information. At WSNS, a light-weight detection of spoofing attacks in wireless networks was presented [15].

Finally, a distributed node revocation approach based on cooperative security has been proposed [23]. Its main objective is the exclusion of compromised or misbehaving nodes from the normal network operation.

4. Conclusion

As can be seen from this retrospection, the IEEE International Workshop on Wireless and Sensor Networks Security (WSNS) has become a interesting event well recognized in the community. According to the received contributions from all around the world, authors see this workshop as a place to discuss high quality research. Thus, WSNS become a forum for all security interested people working in the fields of wireless and sensor networks.

Recently, the trend towards improved service quality in wireless networks raised major interest in the wireless networking domain. Buzzwords are low-latency networking, delay and disruption tolerant networking, and zero-loss

communication. All the techniques developed in these areas have not yet considered to be integrated with security measures. So, new research objectives can be set in these directions.

Additionally, future research issues will still need to focus on the topics reviewed in this retrospection. Secure communication, key management, attack detection, and other issues are not yet solved properly. It seems that application and scenario dependent solutions are required, especially in low resource sensor networks.

WSNS will continue to support the exchange of ideas among interested researchers by providing the right forum and the right environment. We are looking forward to receiving comments, suggestions, and, of course, contributions.

Acknowledgments

We want to thank Prof. Jie Wu for helping us initiating this workshop, the active members of the TPC, the countless reviewers, and, above all, the authors who continuously contributed to WSNS.

References

[1] A. Achtzehn, Z. Benenson, and C. Rohner. Implementing Agreement Protocols in Sensor Networks. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 858–863, Vancouver, Canada, October 2006.

[2] A. Achtzehn, C. Rohner, and I. Rodhe. ARPD: Asynchronous random key predistribution in the LEAP framework for Wireless Sensor Networks. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[3] G. Ács, L. Buttyán, and I. Vajda. The Security Proof of a Link-state Routing Protocol for Wireless Sensor Networks. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[4] C.-C. Chang, D. J. Nagel, and S. Muftic. Assessment of Energy Consumption in Wireless Sensor Networks: A Case Study for Security Algorithms. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[5] S. Chapkin, B. Bako, F. Kargl, and E. Schoch. Location Tracking Attack in Ad hoc Networks based on Topology Information. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 870–875, Vancouver, Canada, October 2006.

[6] X. Chen and J. Drissi. An Efficient Key Management Scheme in Hierarchical Sensor Networks. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[7] Y. Cho and L. Bao. Secure Access Control for Location-Based Applications in WLAN Systems. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 852–857, Vancouver, Canada, October 2006.

[8] F. Dressler. Reliable and Semi-reliable Communication with Authentication in Mobile Ad Hoc Networks. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, pages 781–786, Washington, DC, USA, November 2005.

[9] Z. Jiang, J. Wu, and A. Agah. Topology Control for Secured Coverage in Wireless Sensor Networks. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[10] Q. Jing, J. Hu, and Z. Chen. C4W: An Energy Efficient Public Key Cryptosystem for Large-Scale Wireless Sensor Networks. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 827–832, Vancouver, Canada, October 2006.

[11] M. Khan, F. Amini, J. Misic, and V. B. Misic. The Cost of Security: Performance of ZigBee Key Exchange Mechanism in an 802.15.4 Beacon Enabled Cluster. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 876–881, Vancouver, Canada, October 2006.

[12] K. Kim, J. Hong, and J. Lim. Fast and Efficient Secure Communication Establishing Mechanism for Aero-wireless Environments. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[13] K. T. Kim and R. S. Ramakrishna. A Level-based Key Management for In-Network Processing in WSNs. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[14] Y. W. Law, L.-H. Yen, R. D. Pietro, and M. Palaniswami. Secure k-Connectivity Properties of Wireless Sensor Networks. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[15] Q. Li and W. Trappe. Light-weight Detection of Spoofing Attachs in Wireless Networks. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 845–851, Vancouver, Canada, October 2006.

[16] Z. Li and J. Garcia-Luna-Aceves. New Non-Interactive Key Agreement and Progression (NIKAP) Protocols and Their Applications to Security in Ad Hoc Networks. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[17] J. Liao and P. Huang. Improved Mechanism for Mobile Location Privacy. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[18] J. Ma, S. Zhang, Y. Zhong, and X. Tong. SeLoc: Secure Localization for Wireless Sensor and Actor Network. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 864–869, Vancouver, Canada, October 2006.

[19] A. Mahmoud, A. Sameh, and S. El-Kassas. Reputed Authenticated Routing for Ad Hoc Networks Protocol (Reputed-ARAN). In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[20] E. Makri and Y. C. Stamatiou. Deterministic key predistribution schemes for mobile ad-hoc networks based on set systems with limited intersection sizes. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 833–838, Vancouver, Canada, October 2006.

[21] M. Manulis. Contributory Group Key Agreement Protocols, Revisited for Mobile Ad-Hoc Groups. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[22] V. B. Misic, J. Fung, and J. Misic. MAC Layer Security of 802.15.4-Compliant Networks. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[23] O. G. Morchon and H. Baldus. Distributed Node Revocation based on Cooperative Security. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[24] N. Nehra, R. B. Patel, and V. K. Bhat. Trust Based Routing in Ad Hoc Network: A Mobile Agent Approach. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[25] U. N. Okorafor, K. Marshall, and D. Kundur. Security and Energy Considerations for Routing in Hierarchical Optical Sensor Networks. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 888–893, Vancouver, Canada, October 2006.

[26] J. Opper, B. DeCleene, and M. Leung. Gateway Subset Difference Revocation. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 839–844, Vancouver, Canada, October 2006.

[27] J. Park, Z. Kim, and K. Kim. State-based Key Management Scheme for Wireless Sensor Networks. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[28] M. Passing and F. Dressler. Experimental Performance Evaluation of Cryptographic Algorithms on Sensor Nodes. In *2nd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'06)*, pages 882–887, Vancouver, Canada, October 2006.

[29] K. Pongaliur, C. Wang, and L. Xiao. Maintaining Functional Module Integrity in Sensor Networks. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[30] I. Rodhe, C. Rohner, and A. Achtzehn. n-LQA: n-Layers Query Authentication in Sensor. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[31] S. Schaust, M. Drozda, and H. Szczerbicka. Impact of Packet Injection Models on Misbehaviour Detection Performance in Wireless Sensor Networks. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[32] D. Singelee and B. Preneel. Location Verification using Secure Distance Bounding Protocols. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[33] T. Suen and A. Yasinsac. Peer Identification in Wireless and Sensor Networks Using Signal Properties. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[34] P. Svenda and V. Matyas. Authenticated key exchange with group support for wireless sensor networks. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[35] G. Thamilarasu, A. Balasubramanian, S. Mishra, and R. Sridhar. A Cross-layer based Intrusion Detection Approach for Wireless Ad hoc Networks. In *International Workshop on Wireless and Sensor Networks Security (WSNS'05)*, Washington, DC, USA, November 2005.

[36] L. Tobarra, D. Cazorla, and F. Cuartero. Formal Analysis of Sensor Network Encryption Protocol (SNEP). In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.

[37] L. Zhang, Z. Hu, Y. Ji, and P. Zhang. Grouping-based Clustering Routing Protocol in Wireless Sensor Networks. In *3rd IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'07)*, Pisa, Italy, October 2007.