Wireless Sensor Network Security Visualization

Eirini Karapistoli and Anastasios A. Economides
University of Macedonia
Computer Networks & Telematics Applications Laboratory
Thessaloniki, Greece, GR-54006
{ikarapis,economid}@uom.gr

***Abstract*—Security is becoming a major concern for many mission-critical applications wireless sensor networks (WSNs) are envisaged to support. This is because WSNs are susceptible to various types of attacks or to node compromises that exploit known and unknown vulnerabilities of protocols, software and hardware, and threaten the security, integrity, authenticity, and availability of data that resides in these networked systems. While various security mechanisms have been proposed for these networks dealing with either MAC layer or network layer security issues, or key management problems, the security benefits that can be obtained from an upper visualization layer have not been adequately considered in their design. In this paper, we explore the issues and concerns surrounding the application of visual analysis for wireless sensor network security purposes. This paper focuses on several distinct advantages information visualization and visual analytics can offer in the security domain. In addition, this paper reviews security visualization tools that are available to network security analysts. Finally, it concludes by identifying challenges for this new area of research.**

I. Introduction

WSNs are gaining interest in the research community due to their unique characteristics and the fact that they are potentially low cost solutions to a variety of real-world challenges. A typical WSN comprises a large set of wireless nodes with sensing capabilities, deployed in an ad hoc fashion that coordinate to perform a common task. These nodes are battery-operated devices with limited energy capacity and computational processing capability, requiring mechanisms to minimize their power consumption in order to ensure a long-lasting operation without the need for replacement/recharging the battery. The driving force behind research in WSNs is to develop systems that can operate unattended for years. Because of their potential for physical isolation, this wireless networking technology has a wide range of applications varying from environmental monitoring, to security-oriented ones such as homeland security, military sensing, critical infrastructure protection, and much more [2].

With WSNs being envisioned for use in demanding or even adverse deployment environments, these networks are at risk. Indeed, WSNs are susceptible to various types of attacks or to node compromises that exploit known and unknown vulnerabilities of protocols, software and hardware, and threaten the security, integrity, authenticity, and availability of data that resides in these networked systems [48]. The situation aggravates if we consider that a WSN typically generates a massive large amount of wireless data over its lifetime. This fact escalates the complexity in processing and routing the produced amounts of data, while at the same time it raises severe security issues that mainly stem from the difficulty in identifying network threats that may be lurking in them. All these challenges call for the development of efficient security mechanisms that will safeguard the network's functionality against accidental or operational failures as well as intentional attacks that can lead to sudden and unpredictable changes in network topology, traffic load and capacity of links.

The security of WSNs has been extensively studied by the research community [34], [13], and while there are several open problems that remain to be solved, it is now possible to create a sensor network that complies with a minimal set of security properties. The security recipe necessitates sensor networks to use cryptographic primitives, support key management, integrate security measures into network layer routing protocols, provide with MAC-level authentication and secure data aggregation, and other similar guidelines that come with different implementation difficulties [5].

In general, the security mechanisms that have been proposed for these networks deal with either MAC layer or network layer security issues, or key management problems. Sadly, however, the security benefits that can be obtained from an upper visualization layer have not been adequately considered in their design. Using information visualization and visual analytics a security professional can see the expected and discover the unexpected semantic information that lies within the data, enabling him or her to efficiently integrate automated methods with expert intuition for the detection of complex patterns of abnormal network activity. Based on this notion, this paper explores the potential application of visual analysis for wireless sensor network security purposes. To the best of our knowledge, no similar retrospective studies have been reported in the literature covering the field of wireless sensor network security visualization.

The remainder of the paper is organized as follows: Sections II and III show how visual analysis can foster better insight in the area of wireless sensor network security monitoring by focusing on several distinct advantages information visualization and the science of visual analytics can offer. Section IV reviews existing security visualization tools that are available to network security experts. Section V pinpoints challenges and directions for future research. Finally, conclusions are given in Section VI.

978-1-4673-2015-3/12/$31.00 ©2012 IEEE

II. Until now...Visualization for Network Traffic Analysis

Information visualization is a technique that has been used for a long time to represent information clearly and effectively through graphical means [37]. The basic purpose of visualization is to create interactive visual representations of the information that exploit human's perceptual and cognitive capabilities of problem solving in order to extract information. This is why a growing body of researchers validates the role of visualization as a new tool of data mining (usually referred to as visual data mining [19]) capable of solving complex problems.

Information visualization has been deployed in different fields and recently in visualizing network data [4]. Network traffic visualization is arguably one of the first directions to take when it comes to understanding, analyzing and finding relevant information in vast amounts of data within a network. To aid the network analysts in this task, researchers have proposed numerous visualization techniques (i.e. scatter plots, color maps or some form of a graph, etc.) [6], [19]. In the field of WSNs, several network visualization tools have been proposed to graphically monitor real-world or simulated sensor network deployments [30]. Existing tools like the Surge [26], MoteView [42], Octopus [16] or the Sensor Network Analyzer (for ZigBee-based WSNs) [33], display network activity between sensor nodes and provide users with live information about the network topology and the collected sensory data in order to enable live debugging of the deployed sensor network. In addition, these tools contain various visualization capabilities in order to make it easy to locate packets of interest and to monitor the network health and performance.

Visualization can be very helpful in analyzing and understanding network simulations as well. A number of network simulators suitable for WSNs (TOSSIM [22], OPNET [27], NS-2 [25], QualNet [29]) have begun to employ visual views to represent the network topology layout and packet level animation. These simulators usually generate huge files containing network traffic data, sensor readings, radio links and topology layout information that eases the task of network analysis from the user perspective.

Although the aforementioned standard data visualization tools add a new aspect of network traffic monitoring, at their current form, they lack the specialized techniques in visualizing security-related data and events. The result is that such tools tend to miss abnormalities of the wireless sensor nodes and security attacks that occur unpredictably. This fact strengthens our viewpoint that the ultimate goal of network traffic visualization is fulfilled when the network analyst through that visualization is not only able to monitor the traffic, but can also discriminate between normal, and abnormal activities. We analyze this requirement in the subsequent section, highlighting the need for carefully implementing intelligent analytic components into network visualization systems.

III. In the near future...Visualization for Network Security

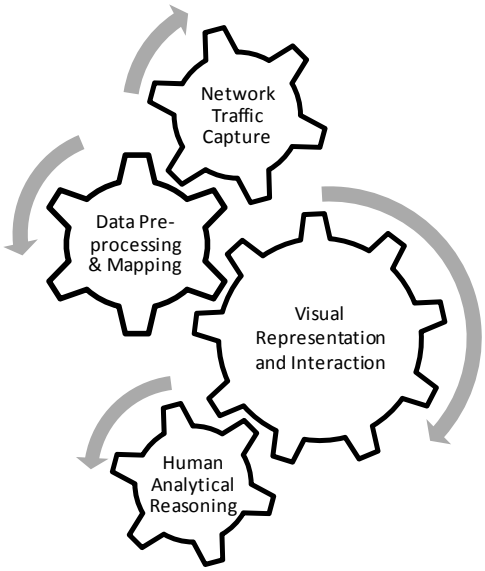

Fig. 1. Generic steps to the visual analysis of network traffic data.

A. The power of Visual Analytics

Indeed, the power of visualization should go beyond the simple "illustration" of network behavior in order to help the analyst to discriminate between normal, and anomalous[1] behavior hidden in a network. Because of this requirement, visualization for network security emerged as an important research topic. The ultimate goal of network security visualization is to provide a network administrator with visual information that will enable him or her to speed up the time it takes to detect, recognize, and analyze a network security event [11]. Several researchers have been studying how visualization can supplement traditional, automatic data mining and analysis methods, which often fail to handle the scale and complexity of the security-related data [43], [47]. Recently, and in order to meet the inherent analytical needs, the scientific community turned to the Visual Analytics approach.

Visual Analytics can be described as "the science of analytical reasoning facilitated by interactive visual interfaces" [39]. It is a tight integration of visual and automatic data analysis methods for information exploration and scalable decision support. Whenever machine learning algorithms become insufficient for recognizing malicious patterns, advanced visualization and interaction techniques can be used as a bridge, encouraging the expert user to explore the relevant data and to take advantage of the human perception, intuition, and background knowledge.

In achieving this objective, visual analytics encompass the following techniques (some of them are shown in 1); 1) *analytical reasoning*, techniques that allow users to obtain deep insights on large data sets; 2) *visual representations and interaction techniques* that enable users to see, explore, and

[1] In general, an anomaly represents a deviation from normalcy. Within this paper, the term *anomaly, abnormal, irregular*, etc., is used interchangeably.

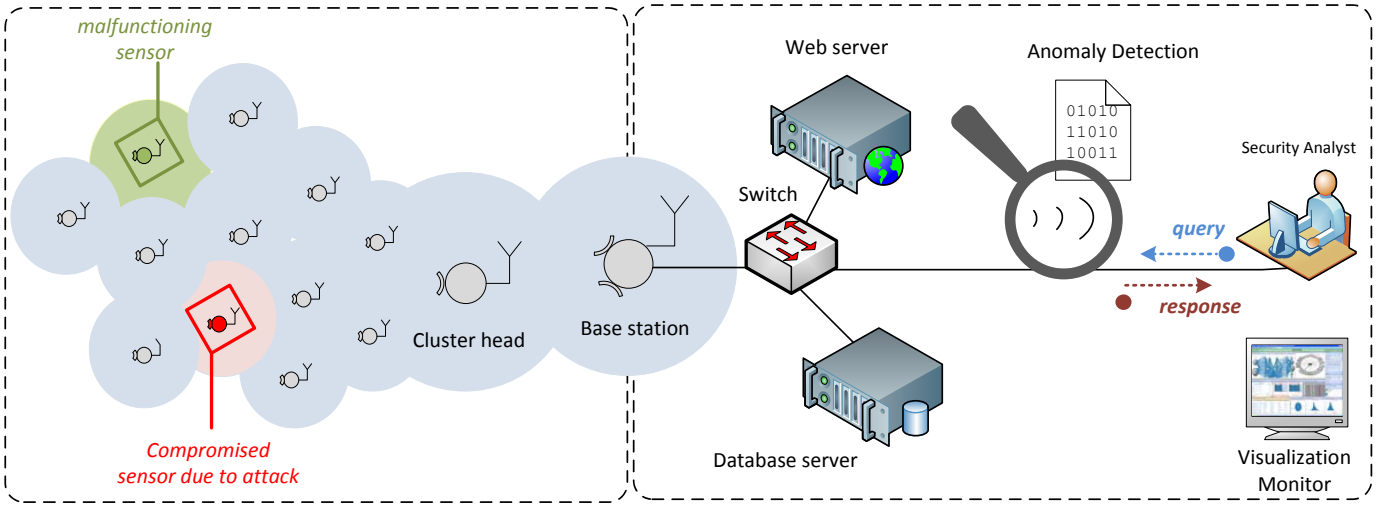

Fig. 2. Architecture of a generic wireless sensor network security visualization system

understand large amounts of information simultaneously; 3) *data representations and transformations* that convert all types of input data in ways that support visualization and analysis; and 4) techniques to support *production, presentation, and dissemination* of analytical results to convey information to audiences [40].

B. Added Features to Network Security

Prior to analyzing the features the visual analytics domain brings to network security, we schematize the architecture of a generic wireless sensor network security visualization system (see Fig. 2). The envisaged system provides the security analyst with real-time visualization of the network traffic generated by the wireless nodes along with security-related data and events, i.e. outliers, correlations changes, etc. Through the visual exploration of the network traffic data and the application of cutting-edge anomaly analytics algorithms, the system administrator would be able to uncover hidden patterns of data, identify emerging vulnerabilities and attacks, and respond decisively with countermeasures that are far more likely to succeed than conventional methods. Because of these features and in contrast to link-layer and network-layer security protection or key management mechanisms that try to prevent successful attacks, such a system targets the identification of attacks and network problems after their occurrence acting as a visual-based intrusion detection system. In this sense, it is complementary to protection-based and prevention-based approaches.

The question however remains. How does visual analytics facilitate the detection of network flaws and anomalies? The use of visualization-based data mining methods for anomaly detection began with the realization that widely-used signature-based methods were too rigid to discover novel attacks[2]. Another problem with signature-based methods is the necessity for time-consuming human input. In contrast, visual analytics successfully incorporate information visualization and machine learning techniques to improve data mining and deal with the complexity of network anomaly detection. This is confirmed by a number of researches which proved that by utilizing the human perception, the identification of unexpected features in the provided visual displays is simplified [38].

Most of the work done in visualization-based anomaly detection stems from the area of computer security [7]. Among the first sophisticated techniques dealing with time series data visualization of network graphs were the Parallel coordinates [7], [14], the star coordinates [18], and the axes-based visualizations with radial layouts [41]. Other studies [23], extend the concept of treemap layouts by proposing an interactive Hierarchical Network Maps (HNMaps) visualization in order to reveal large-scale distributed attacks on Internet traffic. Recently, and in the setting of sensor networks, Shi *et al.* [35] proposed the Temporal Expansion Model (TEM) graph for visually analyzing spatiotemporal anomalies in sensor networks. For an exhaustive overview on network security visualization systems and their anomaly analytics algorithms, the reader can refer to the recent work of Shiravi [36].

Figures 3 and 4 showcase how two selected security visualization tools can make pattern detection easier (attack patterns, in particular). In principle, different types of attacks in WSNs show different behaviors, and as such visualizations of this type are tasked with displaying the different visual patterns. Moreover, many types of attacks are carried out in multiple phases, generally starting with reconnaissance, followed by scanning, acquiring access, maintaining access, and finally clearing tracks and installing back doors for future access. Accordingly, visualizations of this type are also aimed at displaying these phases.

In our paradigms now, and more specifically in Fig. 3a, a circular layout is employed to visualize alert instances [10]. The VisAlert visualization W^3 concept is based on the notion that an alert must possess three attributes namely: *what*, *when*,

[2]For a taxonomy on general non visual-based anomaly detection methods, the reader can refer to the works of Rajasegarar [32] and Jurdak [17].

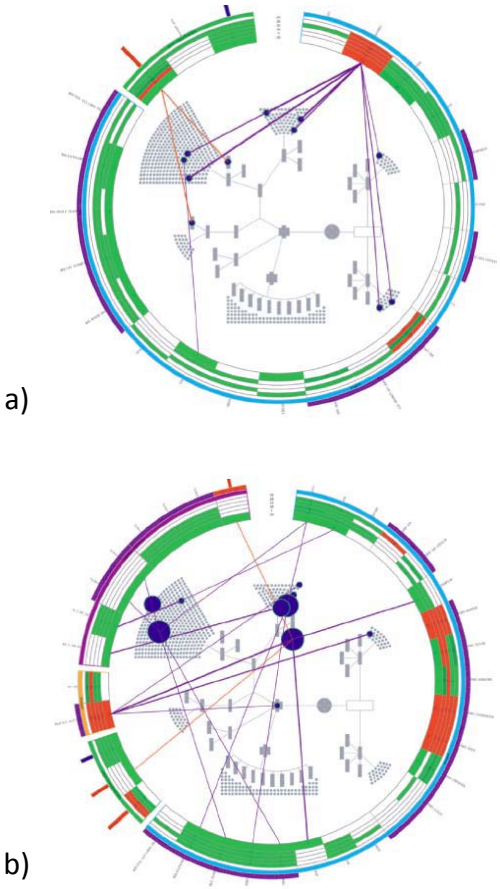

Fig. 3. Visualizing alerts using the VisAlert radial view a) normal activity, b) attack on specific machines [10].

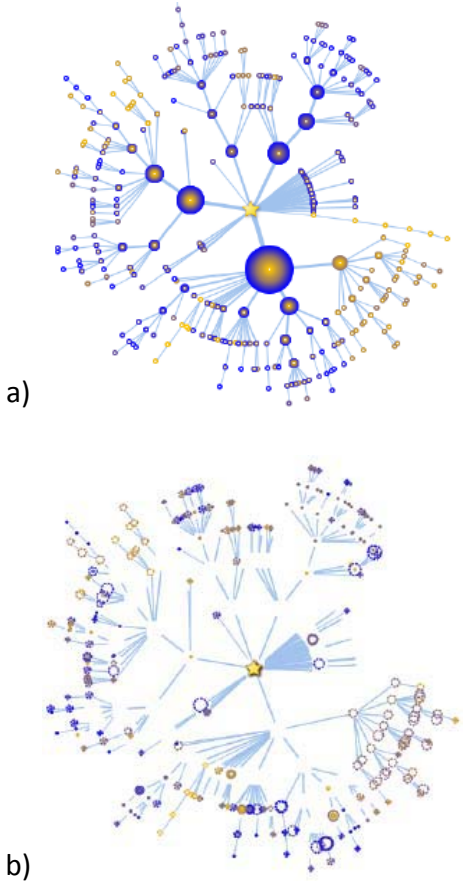

Fig. 4. Visualizing sensor network routing topologies and their anomalies using the TEM graph view of SAVE a) flat TEM and b) flat TEM with anomaly rings [35].

and *where* and that these attributes can be used as a basis for comparing heterogeneous events. As depicted in Fig. 3b, the local network topology map is displayed in the center with the various alerts being attached on a surrounding ring. The ring's width represents time and is divided into several history periods. A line is drawn from an alert type on the outer ring to a particular host on the topology map to represent a triggered alarm. Thicker lines show a higher number of alerts of a single type, and larger nodes in the topology map represent hosts experiencing unique alerts.

In the second paradigm, the topology view of Fig. 4a shows the TEM graph generated from the sensor network routing paths [35]. As the input TEM graph is a directed tree, the authors employ the traditional radial layout to place the sensor nodes. The packet sending pattern is surfaced to the graph similar to the idea of the GrowthRingMap [3], while the temporal anomaly changes within each node are drawn by anomaly rings, as shown in Fig. 4b. As it can be seen, it is more clear that the top right node cluster is counterpart of the cluster in bottom right after the major route change, because their anomaly rings have the same color hue.

The first snapshots of these two powerful visual analytics paradigms seem very promising. It is easy to witness that their well-designed user interfaces provide deep insight into the attack detection process aiding the administrator in his/her security tasks, namely in the detection of anomalous and intrusive behaviors inside a network.

IV. Existing Security Visualization Tools

Though an area in the infancy stage, several visualization tools have been proposed so far by researchers and practitioners for analyzing the security of WSNs during their operation. Sensor Anomaly Visualization Engine (SAVE) [35] proposed by Shi *et al.* is a representative approach to sensor anomaly detection through visualization (see Fig.3). It constitutes an integrated system for anomaly detection in sensor networks using visual analytics technologies. The system fully leverages the power of both visualization and anomaly detection analytics to guide the user to quickly and accurately diagnose sensor network failures and faults. The SAVE system encompasses three distinct procedural phases; a) data preprocessing, including cleansing, structuring and normalization of the data, b) anomaly detection through a cluster-based spatiotemporal mapping of sensor nodes' properties on a centroid (data points that deviate from the centroid are identified as outliers), and c) multi-view visualization, including sensor network routing

topology view, correlation-based projection views for high-dimensional sensor properties, and dimension projection view.

Similarly, Wang and Bhargava [44] proposed a security-enhancing visualization mechanism, called MDS-VOW (Multi-Dimensional Scaling - Visualization Of Wormhole), which is capable of identifying the occurrence of wormhole attacks in static sensor networks. MDS-VOW uses multi-dimensional scaling to reconstruct the network layout. Then, a surface smoothing scheme compensates the impacts of distance estimation errors on the reconstructed network. Finally, MDS-VOW detects the wormhole by graphically visualizing the anomaly (bending distortion) introduced by the attack on the reconstructed surface. With no wormhole present, the network topology is flat, while a wormhole would be seen as a string pulling different ends of the network together. In a subsequent research, the same authors proposed an effective approach for monitoring and detecting Sybil attacks by integrating network security and visualization methods [45].

Another example is SecVizer [1], a network security visualization tool that is capable of parsing any QualNet-generated traffic trace from both wired and wireless network. SecVizer combines topology visualization (in a three-dimensional perspective) with the parallel coordinate plot technique used by rumint [28] in order to obtain a faster and more effective detection of network vulnerabilities. The malicious activities, including Distributed Denial of Service (DDoS) attacks, port scans as well as host scans, are detected by exploring noticeable traffic patterns at both the network topology window and the parallel plot window.

As apparent, the research efforts in visualizing the security of wireless sensor networks are still at an infancy stage. In contrast, substantial research has already been conducted in the area of visualization for computer security in the last few years [7]. A multitude of commercial and open source security data visualization tools have been developed since then allowing for the exploration of the internet traffic by means of interactive visual displays (e.g. [21], [9], and [12]). Several security visualization solutions have also been proposed for 802.11-like networks [8], [15], [31]. Many of these approaches have been proven to be effective at allowing users to discover malicious activities such as worms, DoS attacks (e.g., Smurf and Mailbomb) as well as probing attacks (e.g., Portsweep and IPsweep).

Though powerful the aforementioned solutions are, they are not directly applicable to WSNs because several of the characteristics these networks possess, impose a re-examination of the security visualization problem. The associated challenges to the wireless sensor network security visualization problem are recorded and analyzed in the following section.

V. Research Challenges

The task of applying visual data mining for wireless sensor network security purposes is without doubt a challenging one. The high-dimensional, time-varying and dynamic nature of sensor data, the unpredictable network behavior, and the error-prone transmissions and operations, all bring great challenges that complicate the composition of an analytics-friendly visualization for this type of network. The situation aggravates if we consider that a wireless sensor network typically generates a massive large amount of sensory data over its lifetime, reinforcing the well-known scalability problem the field of visual analytics is also charged with [20].

Another crucial, and at the same time, challenging task is to filter the large amounts of wireless sensory data in such a way that security events stand out. This requirement is followed by the general concern; is it better to use three-dimensional or two-dimensional visualizations? Another difficulty is enabling the visualization to show data for individual sensor nodes while showing data for the entire network to better detect and understand security events. Most of the current network security visualization techniques focus on one of these areas, either displaying data for only one node on a network, or displaying overall network data without going into detail on particular nodes. Without an understanding of the node's traffic significance within the overall network traffic (recall that topological and geographical issues exist in WSNs since the value of data is a function of both time and location), certain types of attacks will be difficult to detect.

Quality of the input data is another problem. Sensor network data have been known for many types of faults, e.g., outliers, spikes, stuck-at and noise [24]. Uncertainty and errors in sensor readings or limitations of the chosen analysis algorithm may produce misleading analysis results. Hence, it is a central issue to find ways to tolerate and automatically detect these faults avoiding the misinterpretation by the security analyst. To face this problem, the notion of sensor data quality, and the confidence of the analysis algorithm needs to be appropriately represented in the visual analytics solutions. Moreover, the user needs to be aware of these data and analysis quality properties at any stage in the data analysis process.

Researchers also need to devise detailed specifications for all types of normal and abnormal activities considered in wireless sensor networks, which in many cases differ from those met in traditional wired and wireless networks. Such a development would in turn assist the attack attribution process, i.e. the process of grouping together attack-related data that are due to the same root cause, and would provide a major improvement to the overall visual representation of the potentially correlated attacks against the WSN. Finally, the contribution of any visualization system needs to be carefully assessed in order to demonstrate the user acceptance and the level of effectiveness and efficiency achieved [46]. We expect that progress will be made on all aforementioned areas.

VI. Conclusions

This paper explored the issues and concerns surrounding the application of visual analysis for wireless sensor network security purposes. While this area of research is still in the infancy stage with several issues already calling for solution, visual analysis can foster better insight by providing several distinct key advantages, namely it a) allows network security professionals to rethink how to recognize risks and protect

against threats, b) enables key aspects of the digital forensic process, including data collection, discovery, investigation, examination, analysis and reporting, and c) offers capabilities for information discovery, processing and visualization tactics. As information visualization and visual analytics become more mature, we expect that these tools will provide an important weapon in the arsenal of security experts and will help towards safeguarding the wireless sensor network's uninterrupted operation against operational failures or intentional attacks.

ACKNOWLEDGMENTS

This work was performed within the framework of the Action "Supporting Postdoctoral Researchers" of the Operational Programme "Education and Lifelong Learning (EdLL)" (Action's Beneficiary: General Secretariat for Research and Technology), and is co-financed by the European Social Fund (ESF) and the Greek State.

REFERENCES

[1] G. Abuaitah and B. Wang. Secvizer: A security visualization tool for qualnet-generated traffic traces. In *Proceedings of the 6th International Workshop on Visualization for Cyber Security (VizSec)*, VizSec '08, pages 111–118, 2009.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless Sensor Networks: A Survey. *Computer Networks*, 38(4):393–422, Mar. 2002.

[3] P. Bak, F. Mansmann, H. Janetzko, and D. Keim. Spatiotemporal analysis of sensor logs using growth ring maps. *Visualization and Computer Graphics, IEEE Transactions on*, 15(6):913–920, nov.-dec. 2009.

[4] S. Card, J. Mackinlay, and B. Shneiderman. *Readings in Information Visualization: Using Vision to Think*. Morgan Kaufmann Publishers, San Francisco, 1999.

[5] X. Chen, K. Makki, K. Yen, and N. Pissinou. Sensor network security: a survey. *IEEE Commun. Surveys Tuts.*, 11(2):52–73, 2009.

[6] E. H. Chi. A taxonomy of visualization techniques using the data state reference model. In *Proceedings of the IEEE Symposium on Information Vizualization 2000*, INFOVIS '00, pages 69–75, Washington, DC, USA, 2000. IEEE Computer Society.

[7] G. Conti. *Security Data Visualization: Graphical Techniques for Network Analysis*. No Starch Press, 1 edition, Oct. 2007.

[8] A. D'Amico, C. Verderosa, C. Horn, and T. Imhof. Integrating physical and cyber security resources to detect wireless threats to critical infrastructure. In *Technologies for Homeland Security (HST), 2011 IEEE International Conference on*, pages 494 –500, Nov. 2011.

[9] F. Fischer, F. Mansmann, D. A. Keim, S. Pietzko, and M. Waldvogel. Large-scale network monitoring for visual analysis of attacks. In *Proceedings of the 5th international workshop on Visualization for Computer Security*, VizSec '08, pages 111–118, 2008.

[10] S. Foresti, J. Agutter, Y. Livnat, S. Moon, and R. Erbacher. Visual correlation of network alerts. *Computer Graphics and Applications, IEEE*, 26(2):48–59, march-april 2006.

[11] M. Gleicher, D. Albers, R. Walker, I. Jusufi, C. D. Hansen, and J. C. Roberts. Visual comparison for information visualization. *Information Visualization*, 10(4):289–309, 2011.

[12] J. Goodall, W. Lutters, P. Rheingans, and A. Komlodi. Preserving the Big Picture: Visual Network Traffic Analysis with TNV. In *Visualization for Computer Security, IEEE Workshops on*, pages 47–54, 2005.

[13] F. Hu and N. K. Sharma. Security Considerations in Ad Hoc Sensor Networks. *Elsevier Ad Hoc Networks*, 3(1):6989, Dec. 2005.

[14] A. Inselberg. The plane with parallel coordinates. *The Visual Computer*, 1:69–91, 1985.

[15] C. Y. Jeong, B. H. Chang, and J. C. Na. A Survey on Visualization for Wireless Security. In *Networked Computing and Advanced Information Management, 2008. NCM '08. Fourth International Conference on*, volume 1, pages 129–132, Sept. 2008.

[16] R. Jurdak, A. G. Ruzzelli, A. Barbirato, and S. Boivineau. Octopus: monitoring, visualization, and control of sensor networks. *Wireless Communications and Mobile Computing*, 11(8), 2011.

[17] R. Jurdak, X. R. Wang, O. Obst, and P. Valencia. *Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies*, chapter 12, pages 309–325. Intelligence-based Systems Engineering. Springer, 2011.

[18] E. Kandogan. Visualizing multi-dimensional clusters, trends, and outliers using star coordinates. In *Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining*, KDD '01, pages 107–116, New York, NY, USA, 2001. ACM.

[19] D. A. Keim. Information Visualization and Visual Data Mining. *IEEE Transactions on Visualization and Computer Graphics*, 8(1):1–8, Jan. 2002.

[20] D. A. Keim, F. Mansmann, J. Schneidewind, J. Thomas, and H. Ziegler. Visual data mining. In S. J. Simoff, M. H. Böhlen, and A. Mazeika, editors, *Visual Analytics: Scope and Challenges*, pages 76–90. Springer-Verlag, 2008.

[21] K. Lakkaraju, R. Bearavolu, A. Slagell, W. Yurcik, and S. North. Closing-the-Loop in s. In NVisionIP: Integrating Discovery and Search in Security Visualization. In *Visualization for Computer Security, IEEE Workshops on*, pages 75–82, 2005.

[22] P. Levis, N. Lee, M. Welsh, and D. Culler. Tossim: Accurate and scalable simulation of entire tinyos applications. In *Proceedings of the 1st international conference on Embedded networked sensor systems (ACM SenSys 03)*, page 5160, Los Angeles, CA, USA, 2003. ACM Press.

[23] F. Mansmann, D. A. Keim, S. C. North, B. Rexroad, and D. Sheleheda. Visual Analysis of Network Traffic for Resource Planning, Interactive Monitoring, and Interpretation of Security Threats. *IEEE Transactions on Visualization and Computer Graphics*, 13:1105–1112, November 2007.

[24] K. Ni, N. Ramanathan, M. N. H. Chehade, L. Balzano, S. Nair, S. Zahedi, E. Kohler, G. Pottie, M. Hansen, and M. Srivastava. Sensor network data fault types. *ACM Trans. Sen. Netw.*, 5(3):25:1–25:29, June 2009.

[25] [Online]. http://isi.edu/nsnam/ns/.

[26] [Online]. http://www.cmt-gmbh.de/surge_network_viewer.htm.

[27] [Online]. http://www.opnet.com/.

[28] [Online]. http://www.rumint.org/.

[29] [Online]. http://www.scalable-networks.com/.

[30] B. Parbat, A. K. Dwivedi, and O. P. Vyas. Article: Data visualization tools for wsns: A glimpse. *International Journal of Computer Applications*, 2(1):14–20, May 2010. Published By Foundation of Computer Science.

[31] K. Prole, J. R. Goodall, A. D. D'Amico, and J. K. Kopylec. Wireless Cyber Assets Discovery Visualization. In *Proceedings of the 5th International workshop on Visualization for Computer Security*, VizSec '08, pages 136–143, Berlin, Heidelberg, 2008. Springer-Verlag.

[32] S. Rajasegarar, C. Leckie, and M. Palaniswami. Anomaly detection in wireless sensor networks. *Wireless Communications, IEEE*, 15(4):34–40, 2008.

[33] N. Sénéchal, S. Hong, and P. Eades. *Display of sensor networks: a feasibility study*. Daintree Networks, july 2006.

[34] E. Shi and A. Perrig. Designing Secure Sensor Networks. *IEEE Wireless Commun. Mag.*, 11(6):3843, Dec. 2004.

[35] L. Shi, Q. Liao, Y. He, R. Li, A. Striegel, and Z. Su. SAVE: Sensor anomaly visualization engine. In *Visual Analytics Science and Technology (VAST), 2011 IEEE Conference on*, pages 201–210, oct. 2011.

[36] H. Shiravi, A. Shiravi, and A. Ghorbani. A Survey of Visualization Systems for Network Security. *Visualization and Computer Graphics, IEEE Transactions on*, 1(99):1–19, 2011.

[37] R. Spence. *Information Visualization - Design for Interaction*. Pearson Educations, 2nd edition, 2006.

[38] S. T. Teoh, K.-L. Ma, S. F. Wu, and T. J. Jankun-Kelly. Detecting flaws and intruders with visual data analysis. *IEEE Comput. Graph. Appl.*, 24(5):27–35, Sept. 2004.

[39] J. J. Thomas and K. A. Cook. *Illuminating the Path: The Research and Development Agenda for Visual Analytics*. National Visualization and Analytics Ctr, 2005.

[40] J. J. Thomas and K. A. Cook. A Visual Analytics Agenda. *IEEE Computer Graphics and Applications*, 26:10–13, 2006.

[41] C. Tominski, J. Abello, and H. Schumann. Axes-based visualizations with radial layouts. In *Proceedings of the 2004 ACM symposium on Applied computing*, SAC '04, pages 1242–1247, New York, NY, USA, 2004. ACM.

[42] M. Turon. MOTE-VIEW: A Sensor Network Monitoring and Management Tool. In *Embedded Networked Sensors, 2005. EmNetS-II. The Second IEEE Workshop on*, pages 11–18, May 2005.

[43] J. van Wijk. The value of visualization. In *Visualization, IEEE, (IEEE VIS'05)*, pages 79–86, oct. 2005.

[44] W. Wang and B. Bhargava. Visualization of wormholes in sensor networks. In *ACM workshop on Wireless Security*, page 5160, New York, NY, USA, 2004. ACM Press.

[45] W. Wang and A. Lu. Visualization assisted detection of Sybil attacks in Wireless Networks. In *Proceedings of the 3rd international workshop on Visualization for computer security*, VizSEC '06, pages 51–60, 2006.

[46] Y.-T. Wang and R. Bagrodia. Sensec: A scalable and accurate framework for wireless sensor network security evaluation. In *Distributed Computing Systems Workshops (ICDCSW), 2011 31st International Conference on*, pages 230–239, june 2011.

[47] J. S. Yi, Y.-a. Kang, J. T. Stasko, and J. A. Jacko. Understanding and characterizing insights: how do people gain insights using information visualization? In *Proceedings of the 2008 conference on BEyond time and errors: novel evaLuation methods for Information Visualization*, BELIV '08, pages 4:1–4:6, New York, NY, USA, 2008. ACM.

[48] Y. Zhou, Y. Fang, and Y. Zhang. Securing wireless sensor networks: a survey. *IEEE Commun. Surveys Tuts.*, 10(3):6–28, 2008.