Sensors & Transducers, Vol. 192, Issue 9, September 2015, pp. 9-15

Sensors & Transducers

http://www.sensorsportal.com

Security in Visible Light Communication: Novel Challenges and Opportunities

[1] Christian ROHNER, [2] Shahid RAZA, [3] Daniele PUCCINELLI, and [1, 2] Thiemo VOIGT

[1] Uppsala University, Dept of Information Technology, Box 337, 75105 Uppsala, Sweden
[2] SICS Swedish ICT, Box 1263, 164 29 Kista, Sweden
[3] SUPSI, Institute for Information Systems and Networking, Via Cantonale, 6928 Manno, Switzerland
[1] Tel.: +46 70 167 9361
[1] E-mail: christian.rohner@it.uu.se

Received: 31 July 2015 /Accepted: 31 August 2015 /Published: 30 September 2015

Abstract: As LED lighting becomes increasingly ubiquitous, Visible Light Communication is attracting the interest of academia and industry as a complement to RF as the physical layer for the Internet of Things. Aside from its much greater spectral availability compared to RF, visible light has several attractive properties that may promote its uptake: its lack of health risks, its opportunities for spatial reuse, its relative immunity to multipath fading, its lack of electromagnetic interference, and its inherently secure nature: differently from RF, light does not penetrate through walls. In this paper, we outline the security implications of Visible Light Communication, review the existing contributions to this under-explored space, and survey the research opportunities that we envision for the near future. *Copyright © 2015 IFSA Publishing, S. L.*

Keywords: Visible light communication, Security.

1. Introduction

With Visible Light Communication (VLC), visible light is employed as the transmission medium and Light Emitting Diodes (LEDs) can offer high-capacity wireless data transmission capabilities on top of the basic role as lighting devices [1]. LEDs are replacing incandescent light bulbs because of their much higher energy efficiency, superior reliability, and ever dropping price points. As LEDs become increasingly ubiquitous, VLC continues to evolve from its former role as a subfield of Optical Wireless Communication to a candidate physical layer for the Internet of Things (IoT) that attracts the attention of both academia and industry. Nowadays, VLC is primarily viewed as a complement to RF in the face of the looming spectrum crunch: as the radio spectrum becomes increasingly crowded, the superior spectral availability in the visible light range becomes increasingly attractive for the IoT with its billion devices that need to be networked.

The bulk of the recent work on VLC has targeted the high end segments of the design space, pursuing the goal of high throughput by means of advanced modulation schemes. Until recently, Gbps range data rates had only been demonstrated with laser diodes [2]; as recently as 2014, a 3 Gb/s link has been demonstrated with a Gallium Nitride LED [3]. Increasing the throughput for visible light is also possible by Multiple-Input-Multiple-Output transceivers as discussed by Azhar, *et al.* [4] and O'Brien, *et al.* [5] whereas Komiyana, *et al.* [6] increase the throughput by using RGB-LEDs with multiple colors such as blue, green and red. Other

authors have explored low-end communication links between resource-constrained devices, using simple LEDs for transmission and LEDs or photodiodes for reception [7-8]. Furthermore, smartphone-based VLC between a screen and a camera has also been explored in recent years [9-11]. At the application layer we have a number of interesting approaches making use of visible light ranging from indoor localization [12-13] to underwater networking with light [14]. Localisation is a key enabler of the IoT as many IoT applications require accurate localization information.

Visible light has several key properties that we review in Section II; while its spectral availability is certainly the main reason behind the growing interest in VLC, the inherent security that stems from the spatial confinement of light beams is arguably the most captivating difference with respect to RF and, quite possibly, the most underrated. In fact, at the time of writing, there are only a few studies that address security in visible light communication. Mostafa and Lutz address secure VLC link at the physical layer [15] by investigating the achievable secrecy rates for of the Gaussian wiretap channel. Zhang, *et al.* [16] propose a secure system for barcode-based VLC, i.e., for secure transmission between a screen and a camera. For supporting a secure data exchange, the system requires a fully duplex VLC channel.

In this paper, we outline the security implications of visible light and we survey the opportunities for VLC security research that arise in the IoT realm. The remainder of the paper is organized as follows. In Section 2, we present the physical layer properties of visible light. Section 3 discusses how to secure visible light communication whereas the following Section 4 takes up security implications of visible light communication. Finally, Section 5 concludes the paper.

2. Physical Layer Properties of Visible Light

VLC was already a key communication tool long before the digital revolution of the past century. Alexander Graham Bell's photophone, patented in 1880, predated Guglielmo Marconi's wireless radio by over 15 years before carried human speech by way of mechanically modulated sunlight. Today's fiberoptic communications networks are based on pulsed light transmitted via glass fibers. IBM Zurich built an optical wireless system as early as the early 1980s, but the technology failed to take off owing to the lack of demand (the Internet was still in its infancy). When wireless communication took off in the 1990s, RF was the wireless medium of choice.

Now that the tightly regulated RF spectrum is getting increasingly crowded, VLC is gaining appeal as a much needed alternative to RF for Internet connectivity. VLC's attractiveness is largely due to the availability of approximately 670 THz of free unlicensed spectrum, which means that very high data rates may be achieved with VLC and, even more importantly, that VLC offers a viable solution to alleviate the spectrum crunch. At the same time, the rise of VLC is also being fueled by the massive uptake of Light Emitting Diodes (LEDs), which are replacing incandescent illumination solutions due to their comparatively high energy efficiency and ever decreasing price points.

The key features of VLC that are advantageous compared to RF and that make VLC an attractive infrastructure for the IoT are:

- Spectral availability (10,000 times larger than RF's with an area spectral efficiency (bits/s/m^2) that is 1,000 greater [17]);
- Free unlicensed spectrum;
- Inherent security due to spatial confinement of light beams (light does not penetrate through walls);
- Spatial reuse opportunities, also due to spatial confinement;
- Immunity to multipath fading;
- Due to the limited Field of View of LEDs, VLC is inherently more directional than RF, and today's commodity hardware may be largely regarded as directional;
- The properties above also enable accurate localization [12-13] and gesture recognition based on visible light [43];
- Non-line-of-sight communication is possible thanks to diffused reflection, provided that the receiver has sufficient sensitivity to detect it;
- Lack of electromagnetic interference;
- Lack of health risks [18].

Most of the academic research on VLC has targeted the high-end portion of the design space, focusing on the achievement of high data rates. Resource-hungry high-end VLC systems have been investigated extensively in a relatively large body of work that has focused on Physical Layer advancements [19-21]. Energy efficiency has not been treated as a first-order problem because the idea is to piggyback on solid state lighting systems so that the communication footprint is negligible compared to the overall lighting footprint. At the time of writing, the provision of Internet connectivity is the most widely cited application of VLC. Dubbed LiFi, VLC-based Internet connectivity is particularly suitable to any application that requires lots of downlink bandwidth and minimal upstream capacity, such as those video/audio download/streaming applications that are taking a massive toll on cellular capacity. The typical architecture is based on Power Line Communication systems to deliver data to light fixtures for VLC forwarding to end devices. This is a particularly advantageous way to offer Internet connectivity in locales where RF is off limits, such as airplanes, operating theaters in hospitals, and hazardous factory environments.

In recent years, the huge potential of optical wireless communication for in-house networking has been practically demonstrated in the EU-funded project OMEGA, achieving rates in the order of Gbps with laser diodes [2]. Data rates of the order of hundreds of Mbps can be achieved with white LEDs

by way of resource-rich hardware with strong computational capabilities [22]. Due to the rising popularity of VLC, the IEEE has recently published a VLC standard for local area networks (IEEE 802.15.7) that defines the Physical and Medium Access layers for short range wireless optical communication using visible light [23] in point-to-point communication scenarios, which have been the primary target of all research efforts in this space thus far and that also present the first step towards VLC as an infrastructure for the IoT.

3. Securing Visible Light Communication

In real-world Internet of Things deployments, wireless communication is usually protected against unauthorized access to the wireless medium, modification of messages, eavesdropping, and replay attacks. Authentication security services confirm the identity of an entity and grant access to the wireless medium. Confidentiality services ensure that only the participating devices understand the contents of messages. Integrity services ensure that the data is not modified while in transit. Last but not least, freshness security services validate that the received data is not a reply of previously received message but that it belongs to the current secure session. There exist three well-known security mechanisms that can be used to protect VLC: proximity-based protection, steganographic protection, and cryptographic protection. These solutions provide security in fundamentally different ways; the choice of any of these solutions for a real-world deployment depends on the application's security requirements.

3.1. Proximity-based Protection

Proximity-based protection relies on the directionality properties of visible light and the inherent confinement of light beams within enclosed spaces; these properties may be exploited to restrict the communication coverage to a specific area. Fine-grained control of light characteristics can limit the flow of communication in a restricted proximity. Such a security solution is acceptable in physically protected environments that offer snoop-free line-of-sight communication. Examples of such environments are enclosed spaces such as rooms and vehicles. Cui, *et al.* [24] discuss some of the key issues in line-of-sight VLC system design.

Ensuring a snoop-free confinement of light signal to a particular source is an open research challenge and having such guarantees offers novel applications and opportunities such as VLC-based access control.

3.2. Steganographic Protection

Steganography aims to protect the communication by hiding a message within another message. A possible steganographic protection is hiding secret communication in existing illumination. Unlike cryptographic protection, stenographically protected messages do not seek attention, e.g., from the NSA, and easily pass casual scrutiny. In a typical steganographic protection scheme, the communicating end points share a secret that describes how data is concealed. Steganography mainly addresses confidentiality, but not authentication and integrity. Nevertheless, it is hard for an attacker (without knowing the shared secret) to breach integrity unless the attacker modifies the entire message and hereby also modifies the hidden message. However, if the confidentiality is compromised, the integrity is also compromised since an attacker can identify and alter the hidden message. This is not the case in cryptography. Providing steganographic protection by hiding secret light signals in existing VLC is worth investigating especially for devices that have limited processing and memory resources and cannot afford to run complex and expansive cryptographic operations.

3.3. Cryptographic Protection and Key Generation

Unlike steganography, cryptography offers most security services including confidentiality (encryption/decryption), integrity (with hashing and message integrity codes), and authentication (identity validation). In the case of VLC, cryptographic protection can be applied at different layers. The IEEE 802.15.7 standard for VLC already provides confidentiality and integrity security services at the MAC layer. The security is optional and no key management is specified in 802.15.7; however, standardization efforts are being carried out in the new IEEE 802.15.9 WG to provide key management for 802.15.4 and 802.15.7. Schmid, *et al.* [7] provide MAC and physical layers for LED-to-LED VLC networks but propose the implementation of security at the upper layers.

Modern cryptographic protection mainly relies on secret keys and all other operations are known, i.e., security through obscurity is avoided. Key management, however, is one of the hardest problems in cryptography. Solutions have been proposed that exploit the properties of wireless channels to generate keys to secure wireless links [25-26]. For instance, it is possible to exploit channel reciprocity, whereby two closely located receivers experience the same signal envelope in the absence of interference [27]. Since practical channels are never immune to interference, a technique is presented in [25] that does not require identical signal envelopes for the communicating terminals, but only matching deep fades, which are immune to reasonable levels of interference.

Because the light carrier wavelength is much smaller than the area of the photodetector, VLC is immune to fast fading and is only subject to slow fading in the form of path loss and log-normal shadowing [1]. Because of VLC's relative immunity

to multi-path fading compared to RF, the effectiveness of schemes based on channel reciprocity for VLC must be thoroughly investigated. In the case of systems using both VLC and RF, it is possible to use the radio for key generation, and then use the generated keys for VLC.

3.4. Chaffing and Winnowing

In addition to the three methods explained above for VLC protection, a less known security mechanism called chaffing and winnowing [28] can also be used. It offers confidentiality and authentication services but without requiring any encryption/decryption. It uses shared key and Message Authentication Codes (MACs) to provide authentication and uses the same MACs to offer confidentiality. For confidentiality, it breaks the message into smaller packets and assigns a serial number to each packet. The sender sends the valid packets as well as chaffs (fake packets) that have a valid serial number and message format but a bogus MAC. The receiver records all the packets that have valid MACs and immediately discards the packets that have invalid MACs; this process is called winnowing. The receiver can assemble the valid packets and recover the secret message. While this technique is underused nowadays, it may be worth to investigate the use of chaffing and winnowing in VLC. Steganography and chaffing and winnowing are alternative candidates in situations where export control or other circumstances hinder the use of cryptography.

4. VLC Security: Attacks and Opportunities

In this section we highlight opportunities and attacks in the context of VLC security. Opportunities arise through the use of VLC as out-of-band or side-channel, and the physical properties of light. Attacks known from radio communication get a different flavor in VLC, mainly because of the restricted Field of View of LEDs. This includes jamming, a denial-of-service attack that is a particular threat to mission-critical IoT systems that must deliver data timely.

4.1. Authentic Channels

An interesting concept in visible light communication are visual channels enabled by the transmission between a screen and a camera. These allow users to recognize and verify the captured scene. Visual channels can be used as a secure out-of-band channel for intuitive pairing of devices using two-dimensional barcodes, displayed by (or affixed to) at least one of the devices. The barcode represents security-relevant information that can be read visually by a camera-equipped device and is used to set up an authenticated channel.

Visual channel are considered resilient against active attacks such as man-in-the-middle attacks, and have the property that active attacks are easily detected by the user. The idea of encoding cryptographic information into barcodes was first proposed by Hanna [29] as well as Gehrmann, *et al.* [30]. This work has be generalized into the concept of visual channels by McCune in his work 'Seeing-is-believing' [31]. Saxena, *et al*. [32] extends the Seeing-is-believing system to achieve mutual authentication using just a unidirectional visual channel, and using visual channel authentication even on devices with limited displaying capabilities (e.g., LEDs). The ability to provide an authentic channel is unique to VLC and is not available in radio communication.

4.2. Out-of Band Channels

Out-of-band channels are an important tool to establish security in general, and have been used in particular for authentication purpose [33]. For example, receiving the same (or complementary) information through independent channels imply higher probabilities for message authentication. The potential ubiquity of VLC makes it an ideal candidate to complement a radio communication channel for security purposes, for instance to distribute public keys or a fingerprint thereof to check the authenticity of key material received over the primary communication channel. [1]

4.3. Multiple VLC Channels

VLC scenarios often include several light sources, potentially offering multiple (out-of-band) channels. If operated interference-free and possibly directed, VLC could create zones in which subsets of the sources can be received. From a security perspective, such zones could be combined with network coding [34] or threshold secret sharing schemes [35] where T out of N linear combinations of data are needed to re-construct it. This can be used to either increase the probabilities for message authentication (see Section IV-B), to make data only accessible in certain spatial zones, or to require the user to move around in a room to collect the necessary information to re-construct the data.

Visible light has the property that the effective intensity of light is additive that is, light from different sources will add upp at the receiver. The received signal will therefore be unique for the location. Besides of being used for localization, this property has been leveraged for distance bounding [36] or key generation [37] in radio communication. Although multi-path fading and dispersion are expected to be

[1] a.k.a. multi-factor authentication

much smaller in VLC, direct on-off modulations will result in distinct timing patterns that can be used for this purpose.

4.4. Denial-of-Service

Denial-of-service attacks based on jamming are relatively straightforward to perform on many wireless networks [38]. In particular, low-power radios are notoriously easy to jam even without sophisticated hardware support [39]. There exist approaches to guard low-power radio networks from malicious traffic. In [40], for instance, a central unit detects and corrupts malicious packets so they are not accepted by the unit under attack. Note that this approach, however, can only detect jamming without preventing it [41]. Another option is to detect and map jammed areas to reroute the traffic around these areas [42], but this is only applicable for larger networks.

As discussed in Section II today's VLC can be regarded as directional which makes it easier to defend against the equivalent of jamming attacks on low-power radios. Fig. 1 presents a scenario where an attacker tries to disturb the sink node from receiving a packet. Note that in this scenario we assume that the attacker uses a directional light source. Furthermore, we assume the attacker knows the position of the node against which it launches the attack, and is therefore able to aim the light beam accurately. Jamming attacks on low-power radios do not need such information and are hence easier to launch. Once the attack is detected, the node under attack could physically shield itself from the attack and a multi-hop visible light network[2] could reroute to deliver information via other nodes to the intended sink as shown in Fig. 1. In networks where transmissions are less directional as is the case for most RF communication that often use omnidirectional antennas, shielding in a similar manner would be much more difficult.

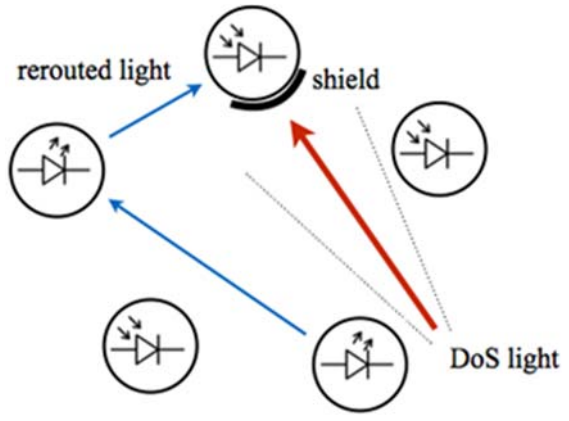

Fig. 1. Visible light DoS defense via shielding and rerouting.

[2] We expect to see such networks multi-hop VLC networks in the future which requires, however, a redesign of the protocol stack.

While in the discussion above we make use of transmitter's directionality to defend against denial-of-service, the same properties also cause problems. For example, as mentioned above, jamming attacks on low-power radio networks can be detected [41]. Due to the multi-path effects and the inherent broadcast nature of radio traffic, a jamming attack on one or several hosts can easily be detected by other nodes that would also experience a higher energy level in the radio channel. These nodes can then take actions such as re-routing of traffic. With today's directional VLC channels, however, it might not be as straightforward to understand that one or several nodes are exposed to a jamming attack. For example, even light sensors close to the host under attack might not recognize an ongoing attack even though a human present in the same room might be able observe such an attack.

5. Conclusions

Thanks to the massive uptake of LEDs for illumination as well as the fear of the RF spectrum crunch, VLC has recently emerged as a hot research area and complement to RF as infrastructure for the IoT. Nevertheless, VLC security has only been investigated in a few studies. In this paper, after reviewing the key properties that make VLC fundamentally different from RF, we have surveyed various solutions from the wired/RF security literature that may be employed successfully to secure VLC. Moreover, we have delved into a survey of opportunities for security research that arise from the uptake of VLC, and we have reasoned about how attacks against VLC may fare. We hope that this paper will serve to stimulate future investigations in VLC security research, which remains an under-explored space whose strategic importance is bound to grow as VLC research and development efforts continue to gain momentum in the IoT realm.

References

[1]. S. Dimitrov, H. Haas, Principles of LED Light Communications, *Cambridge University Press*, 2015.

[2]. OMEGA, the Home Gigabit Access project, http://www.ict-omega.eu.

[3]. D. Tsonev, H. Chun, H. Rajbhandari, J. McKendry, S. Videv, E. Gu, M. Haji, S. Watson, A. Kelly, G. Faulkner, M. Dawson, H. Haas, D. O'Brien, A 3 Gb/s single-LED OFDM-based wireless VLC link using a gallium nitride μLED, *IEEE Photonics Technology Letters*, Vol. 26, No. 7, 2014, pp. 637-640.

[4]. A. H. Azhar, T.-A. Tran, D. O'Brien, Demonstration of high-speed data transmission using MIMO-OFDM visible light communications, in *Proceedings of the IEEE Globecom Workshops (GC'10)*, 2010, pp. 1052-1056.

[5]. D. C. O'Brien, S. Quasem, S. Zikic, G. E. Faulkner, Multiple input multiple output systems for optical wireless: challenges and possibilities, in *Proceedings of the SPIE Optics and Photonics. International Society for Optics and Photonics*, Vol. 6304, 2006.

[6]. T. Komiyama, K. Kobayashi, K. Watanabe, T. Ohkubo, Y. Kurihara, Study of visible light communication system using RGB LED lights, in *Proceedings of the IEEE SICE Annual Conference (SICE)*, 2011, pp. 1926-1928.

[7]. S. Schmid, G. Corbellini, S. Mangold, T. R. Gross, LED-to-LED visible light communication networks, in *Proceedings of the Fourteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'13)*, 2013, pp. 1-10.

[8]. D. Giustiniano, N. O. Tippenhauer, S. Mangold, Low-complexity visible light networking with LED-to-LED communication, *IFIP Wireless Days'12*, Dublin, Ireland, Nov. 2012, pp. 1-8.

[9]. T. Hao, R. Zhou, G. Xing, COBRA: color barcode streaming for smartphone systems, in *Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, 2012, pp. 85-98.

[10]. W. Hu, J. Mao, Z. Huang, Y. Xue, J. She, K. Bian, G. Shen, Strata: Layered coding for scalable visual communication, in *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking (MobiCom'14)*, ACM, 2014, pp. 79-90.

[11]. A. Wang, S. Ma, C. Hu, J. Huai, C. Peng, G. Shen, Enhancing reliability to boost the throughput over screen-camera links, in *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking (MobiCom'14)*, 2014, pp. 41-52.

[12]. P. Hu, L. Li, C. Peng, G. Shen, F. Zhao, Pharos: enable physical analytics through visible light based indoor localization, in *Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks*, 5, 2013, pp. 1-7.

[13]. L. Li, P. Hu, C. Peng, G. Shen, F. Zhao, Epsilon: A visible light based positioning system, in *Proceedings of the 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, Seattle, USA, 2014, pp. 331-343.

[14]. M. Dunbabin, P. Corke, I. Vasilescu, D. Rus, Data muling over underwater wireless sensor networks using an autonomous underwater vehicle, in *Proceedings of the IEEE International Conference on Robotics and Automation* (*ICRA'06*), 2006, pp. 2091-2098.

[15]. A. Mostafa, L. Lampe, Physical-layer security for indoor visible light communications, in *Proceedings of the IEEE International Conference on Communications (ICC)*, 2014, pp. 3342-3347.

[16]. B. Zhang, K. Ren, G. Xing, X. Fu, C. Wang, Sbvlc: Secure barcode-based visible light communication for smartphones, in *Proceedings of the IEEE INFOCOM*, 2014, pp. 2661-2669.

[17]. A. Sevincer, A. Bhattarai, M. Bilgi, M. Yuksel, N. Pal, LIGHTNETs: Smart LIGHTing and Mobile Optical Wireless NETworks, *IEEE Communications Surveys and Tutorials*, Vol. 15, No. 4, 2013, pp. 1-22.

[18]. M. S. Uddin, J. S. Cha, J. Y. Kim, Y. M. Jang, Mitigation technique for receiver performance variation of multi-color channels in visible light communication, *Sensors*, Vol. 11, No. 6, 2011, pp. 6131-6144.

[19]. M. Afgani, H. Haas, H. Elgala, D. Knipp, Visible Light Communication Using OFDM, in *Proceedings of the 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TRIDENTCOM'06)*, Barcelona, Spain, 1–3 March 2006, pp. 129-134.

[20]. R. Mesleh, H. Elgala, H. Haas, Optical Spatial Modulation, *IEEE/OSA Journal of Optical Communications and Networking*, Vol. 3, No. 3, March 2011, pp. 234-244.

[21]. S. Dimitrov, S. Sinanovic, H. Haas, Clipping Noise in OFDM-based Optical Wireless Communication Systems, *IEEE Transactions on Communications (IEEE TCOM)*, Vol. 60, No. 4, Apr. 2012, pp. 1072-1081.

[22]. J. Vucic, C. Kottke, S. Nerreter, K. Langer, J. Walewski, 513Mbit/s visible light communications link based on DMT-modulation of a white LED, *Journal of Lightwave Technology*, Vol. 28, No. 24, Dec. 2010, pp. 3512-3518.

[23]. IEEE Standard for Local and Metropolitan Area Networks 15.7: PHY and MAC Standard for Short-Range Wireless Optical Communication Using Visible Light, IEEE Standard 802.15.7.

[24]. K. Cui, G. Chen, Z. Xu, R. D. Roberts, Line-of-sight visible light communication system design and demonstration, in *Proceedings of the IEEE 7th International Symposium on Communication Systems Networks and Digital Signal Processing (CSNDSP'10)*, 2010, pp. 621-625.

[25]. B. Azimi-Sadjadi, A. Kiayias, A. Mercado, B. Yener, Robust key generation from signal envelopes in wireless networks, in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, Alexandria, VA, USA, 2007, pp. 401-410.

[26]. S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, S. V. Krishnamurthy, On the effectiveness of secret key extraction from wireless signal strength in real environments, in *Proceedings of the 15th Annual International Conference on Mobile Computing and Networking (MobiCom'09)*, Beijing, China, Sep. 2009, pp. 321-332.

[27]. R. Wilson, D. Tse, R. Scholtz, Channel identification: Secret sharing using reciprocity in ultrawideband channels, *IEEE Transactions on Information Forensics and Security*, Vol. 2, No. 3, 2007, pp. 364-375.

[28]. R. L. Rivest, *et al.*, Chaffing and winnowing: Confidentiality without encryption, *CryptoBytes (RSA Laboratories)*, Vol. 4, No. 1, 1998, pp. 12-17.

[29]. S. R. Hanna, Configuring security parameters in small devices, [draft-hanna-zeroconf-seccfg-00], 2002.

[30]. C. Gehrmann, Deliverable Detailed Technical Specification of Mobile Terminal System Security, *SHAMAN*, 2002.

[31]. J. M. McCune, A. Perrig, M. K. Reiter, Seeing-is-believing: using camera phones for human-verifiable authentication, in *Proceedings of the IEEE Symposium on Security and Privacy*, 2002, pp. 110-124.

[32]. N. Saxena, J.-E. Ekberg, K. Kostiainen, N. Asokan, Secure device pairing based on a visual channel, in *Proceedings of the IEEE Symposium on Security and Privacy*, 2006, pp. 313-319.

[33]. L. M. Feeney, B. Ahlgren, A. Westerlund, A. Dunkels, Spontnet: Experiences in configuring and securing small ad hoc networks, in *Proceedings of the 5th Int'l Workshop on Networked Applicances (IWNA5)*, 2002, pp. 102-106.

[34]. R. Ahswede, C. Ning, S.-Y. Li, R. Yeung, Network information flow, *IEEE Transactions on Information Theory*, Vol. 46, No. 4, 2000, pp. 1204-1216.

[35]. A. Shamir, How to share a secret, *Communications of the ACM*, Vol. 22, No. 11, 1979, pp. 612-613.
[36]. S. Brands, D. Chaum, Distance-bounding protocols (extended abstract), *EUROCRYPT'93, Lecture Notes in Computer Science*, Vol. 765, 1993, pp. 344-359.
[37]. R. Blom, An optimal class of symmetric key generation systems, *EUROCRYPT'84, Lecture Nodes in Computer Science*, Vol. 209, 1985, pp. 335-338.
[38]. A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, G. E. Pantziou, A survey on jamming attacks and countermeasures in WSNs, *IEEE Communications Surveys and Tutorials*, Vol. 11, No. 4, 2009, pp. 42-56.
[39]. A. Wood, J. A. Stankovic, G. Zhou, Deejam: Defeating energy-efficient jamming in IEEE 802.15. 4-based wireless networks, in *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, 2007, pp. 60-69.
[40]. M. Wilhelm, I. Martinovic, J. Schmitt, V. Lenders, WiFire: A firewall for wireless networks, in *Proceedings of the ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'11)*, New York, NY, USA, August 2011, pp. 456-457. [Online]. Available: http://discofiles/publicationsfiles/WMSL11- 2.pdf
[41]. D. Giustiniano, V. Lenders, J. B. Schmitt, M. Spuhler, M. Wilhelm, Detection of reactive jamming in DSSS-based wireless networks, in *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2013, pp. 43-48.
[42]. A. Wood, J. A. Stankovic, S. H. Son, JAM: A jammed-area mapping service for sensor networks, in *Proceedings of the 24th IEEE Real-Time Systems Symposium (RTSS'03)*, 2003, pp. 286-297.
[43]. T. Li, C. An, Z. Tian, A. Campbell, X. Zhou, Human Sensing Using Visible Light Communication, in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (MobiCom)*, Paris, France, September 2015.