Hindawi
Security and Communication Networks
Volume 2018, Article ID 2731859, 2 pages
https://doi.org/10.1155/2018/2731859

Editorial

Covert Communication Networks in Hostile Environments

Kiseon Kim,[1] **Jalel Ben-Othman**,[2] **and Prem Mahalik**[3]

[1]*Gwangju Institute of Science and Technology, Gwangju, Republic of Korea*
[2]*University of Paris 13, Villetaneuse, France*
[3]*California State University, Fresno, California, USA*

Correspondence should be addressed to Kiseon Kim; kskim@gist.ac.kr

Received 15 November 2018; Accepted 15 November 2018; Published 2 December 2018

Wireless sensors and multimedia communications are increasingly becoming a part of our everyday lives and societies. Subsequently, issues surrounding their safety and security are becoming ever more important. The situation is true, not only for overtly hostile environments such as for defense and public security, but also for covert commercial platforms handling private and sensitive information.

Also, with the advent of new devices and circuits from the development of military systems, a host of new technologies have come to the fore, including sophisticated RF sensing, activating, signal processing, and communications. The prompt ability to protect against hostile actions to sense, access, process, command, and control covert information is of utmost importance and is vital for the success of this next generation of communication systems and networks.

This special issue presents several research results in covert communication networks in hostile environments, including the identification of current challenges for each domain, the development of novel technologies and strategies, and discussion and exploration of future solutions.

The first challenge of the cover communications and networks is how to confront the hostile noises or environments. Historically, for communication engineers, the white Gaussian is the least favorable noise [1], and conventional system designer considers the best design under the least favorable Gaussian or combination of the multiple or variational Gaussian, such as Rician, Nakagami, or others in [2]. However, the hostile noises are far from the natural Gaussian shape and are rather close to typical signals such as single tone and sweep sinusoidal jamming. Further, the hostile noise is very intentional, having less information in theory in other words. Subsequently, we may fully utilize the known and expectable facts to narrow down the noises and improve the system, compared to that pessimistically designed against the least favorable noses.

Considering diverse conditions and situations for representing the hostile noises and environments, purely analytic approaches are sometimes very limited in applications and modeling and simulation (M&S) approach is a good alternative for the covert communications and networks, where we need a general M&S framework [3]. H. Kang et al. proposed an open architecture framework for covert communications and networks models, especially for military warfare simulations using six components and ten rules. Specific development of a scenario in the electronic warfare domain was demonstrated using distributed simulation interface models and using case models to enable High-Level Architecture (HLA) based real-time distributed simulations with simple C++ and MATLAB Application Programming Interface (API).

More than the presentation of a general M&S framework, S. R. Park et al. investigated radar responses to electronic attacks in electronic warfare environments. Typical detection and communications systems are well analyzed and understood conventionally, Again, however, the hostile noises such as single-tone jamming and sweep jamming need to be fully utilized to further improve the system, compared to that designed against the least favorable noses. They constructed an EW simulator considering the inputs of the characteristic parameters of radar threat, radar warning receiver, jammer, electromagnetic wave propagation, and simulation scenario. Then, they can simulate the feature of radar threats and efficient electronic attacks in electronic warfare.

Covert communication and networks not only transmit multimedia data but also need to convey telemetry and other support data such as time and location of a certain system [4]. In particular, while starting a new communications link, it is very essential for both end systems to synchronize the time-stamp and geolocate a position. For covert communications, these time and position, sometimes additional information of frequency, phase and code, and so forth, are very essentially processed. J.-H. Lee et al. practically considered antenna factors airborne communication system for direction finding. Considering the flying shape of the airplane bodies, proper M&S provided interesting results on how to select the optimum antenna position.

The mission of covert communications and networks is more than the support like signal acquisition, location detection, direction finding and surveillance, and so forth, and two key missions of the covert communications and networks are aggressive attack and preventive protection, that is, electronic attack (EA) and electronic protection (EP) [4]. EA is directly related to the hostile environment, with intentional radiation of the opponents to hinder the friends' communications. B. V. Nguyen investigated a Noncoherent Chaotic Shift Keying (NCSK) system, namely, NR-NCSK, as a state-of-the-art communications system and simulated the antijamming performance under the hostile electronic attack [5]. Through extensive M&S of the jamming and system performance, much known behaviors of single-tone and multitone jamming, and effects of the starting frequency, sweep duration and the sweep bandwidth of the sweep jammer.

For another emerging cognitive radio network (CRN) [5], P.-D. Thanh et al. investigated the effect of the jamming attacks, especially when the physical layer of multihop transmission, the relay energy, is limited and energy harvesting is available, while multiple jamming exists. They simulated the throughput/delay ratio to optimize overall network performance in terms of end-to-end delay, throughput, and energy efficiency, along with devising proper multihop allocation schemes.

So far, physical layer is the main target to simulate the covert communication system, yet more information-theoretic approaches are available at the higher layer such as medium access (MAC) and the upper layers. Consider that the overall optimization is not that easy under a hostile environment and divide-and-conquer approach is an alternative to achieve the near-best performance of the covert communication and networks, especially with a partial information about the noise including a case when there is no information about the jamming. J. Park et al. contributed toward the Reed-Solomon coded SFH/MFSK system over jamming channels. In contrast to conventional erasure insertion schemes, iterative erasure insertion schemes are confirmed via simulations to have the performance improvement using a generalized minimum distance (GMD) decoding method.

The last, but not the least, research covered overtly hostile environments of public transportation. In particular, train control railway communication is an interesting domain where safety and security become more important, while the speed of train and corresponding information increase. When the conventional control cannot meet the requirements deterministically or the control inherently includes ambiguous and vulnerable factors, a new framework of M&S is an alternative to handle this hostile environment. I. Arsuaga et al. investigated new communication technologies for European railway systems. They introduced recent works of vulnerability identification, related to integrity, authenticity, availability, and confidentiality, along with effective countermeasures to mitigate potential vulnerabilities.

It is noteworthy that topics and approaches handled in this issue can be extended further to research on diverse issues, such as advanced covert communication systems, secure communications in hostile environments, countermeasures against covert communication network, system performance modeling and simulation in hostile environments, reliability and survivability for susceptible networks, emerging surveillance techniques using active and passive sensing, advanced networked and agile systems for hostile environments, cooperation-based systems, and cognitive radio networks operating in hostile environments distributed and coherent signal processing for physical security communications, and emerging manned and unmanned covert applications for air, sea, land, and space.

Finally, we express our great appreciation to all contributors for their excellent time and effort to share knowledgeable information, to review and comment for their valuable help, and to organize and support various administrative works. The Lead Guest Editor in Chief would like to specially thank the other two Guest Editors, for their dedicated cooperation. We hope the special issue will bring readers useful academic reference in their research.

Conflicts of Interest

I and other GEs have no conflicts of interest or private agreements with companies.

Acknowledgments

This work was partially supported by the GIST-EWRC Basic Research Program, Korea.

Kiseon Kim
Jalel Ben-Othman
Prem Mahalik

References

[1] K. Kim and G. Shevlyakov, "Why Gaussianity?" *IEEE Signal Processing Magazine*, pp. 102–113, 2008.

[2] M. K. Simon and M. S. Alouini, *Digital Communications Over Fading Channels*, Wiley, 2005.

[3] D. L. Adamy, *Introduction to Electronic Warfare Modeling and Simulation (Electromagnetics and Radar)*, Artech House, 2003.

[4] S. A. Vakin, L. N. Shustov, and R. H. Dunwell, *Fundamentals of Electronic Warfare*, Artech House, 2001.

[5] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Communications Magazine*, vol. 19, no. 6, pp. 106–112, 2012.