Implementing a Broadcast Storm Attack on a Mission-Critical Wireless Sensor Network

Irina Krivtsova[1], Ilya Lebedev[1], Mikhail Sukhoparov[1], Nurzhan Bazhayev[1], Igor Zikratov[1], Aleksandr Ometov[2(✉)], Sergey Andreev[2], Pavel Masek[3], Radek Fujdiak[3], and Jiri Hosek[3]

[1] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University), St. Petersburg, Russia
[2] Tampere University of Technology, Korkeakoulunkatu 10, 33720 Tampere, Finland
aleksandr.ometov@tut.fi
[3] Brno University of Technology, Technicka 3082/12, Brno, Czech Republic

Abstract. In this work, we emphasize the practical importance of mission-critical wireless sensor networks (WSNs) for structural health monitoring of industrial constructions. Due to its isolated and ad hoc nature, this type of WSN deployments is susceptible to a variety of malicious attacks that may disrupt the underlying crucial systems. Along these lines, we review and implement one such attack, named a broadcast storm, where an attacker is attempting to flood the network by sending numerous broadcast packets. Accordingly, we assemble a live prototype of said scenario with real-world WSN equipment, as well as measure the key operational parameters of the WSN under attack, including packet transmission delays and the corresponding loss ratios. We further develop a simple supportive mathematical model based on widely-adopted methods of queuing theory. It allows for accurate performance assessment as well as for predicting the expected system performance, which has been verified with statistical methods.

Keywords: Information security · Ad hoc networks · Multi-agent systems · Vulnerability · Device availability · Prototyping

1 Introduction and Background

The evolution of wireless sensor networks supports increasingly novel and sophisticated applications across various fields [1]. Modern wireless sensor networks (WSNs) find their use in diverse environments, starting with the marine [2] and vehicular [3] through the forestry [4], and towards the growing industrial Smart Cities [5,6]. Generally, the main advantage and the limitation of the WSNs is in their ad hoc nature, which makes them easy to deploy but difficult to manage. Most of the practical WSN deployments are utilizing wireless relaying to the remote control center, which brings a variety of potential vulnerabilities to be exploited.

L. Mamatas et al. (Eds.): WWIC 2016, LNCS 9674, pp. 297–308, 2016.
DOI: 10.1007/978-3-319-33936-8_23

Arguably, the most demanding areas of the WSN research may be shaped by urban and environmental applications [7]. In this work, we focus on a representative urban WSN application for industrial sensing – *structural health monitoring* [8]. This concept allows to maintain the appropriate condition of engineering structures by deploying sensors in the essential parts of buildings and other constructions, i.e. bridges, tunnels, skyscrapers, etc. The main purpose of such a WSN is to notify the control center about any significant change of the monitored object due to earthquakes, disasters, explosions, or other accidents. A secondary function is to provide continuous health monitoring. As a characteristic example, we may consider the Golden Gate Bridge in San Francisco Bay (shown in Fig. 1), where a similar network was deployed 10 years ago [9].

Clearly, a bridge of any kind is an object of national importance and therefore the serving WSN should be protected from the malicious attackers. However, due to the lack of relevant standardization activities, different manufacturing companies are utilizing a variety of dissimilar security solutions across their deployments, thus making them easier to attack. The use of wireless ad hoc sensor networks for critical applications poses novel information security challenges [10,11], such as: channel sniffing [12]; packet spoofing [13]; physical access to the device [14]; non-standardized communications protocols [15], and many others. We face the fact that development, deployment, and management of such a network is limiting the chance to use conventional information security solutions [16–18].

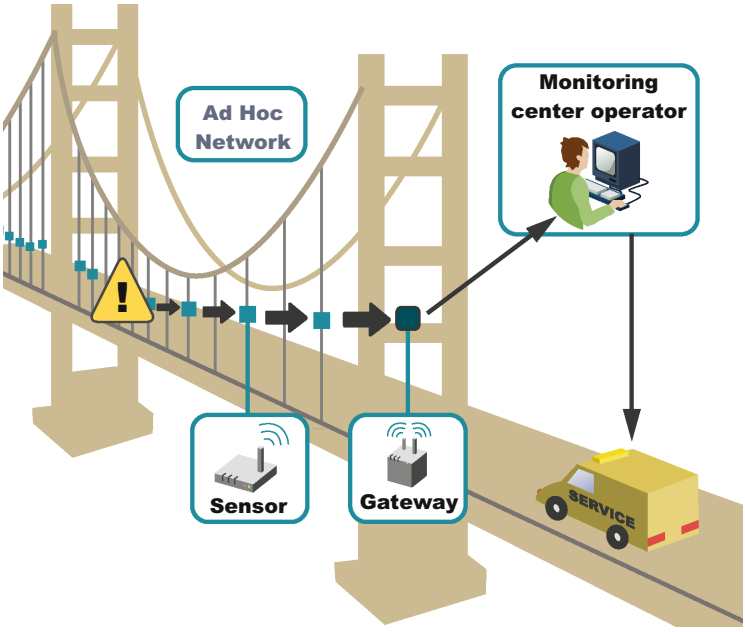


Fig. 1. Example ad hoc WSN deployment for structural health monitoring

In this work, we focus on one of the most threatening attacks on mission-critical WSNs – the broadcast storm [19]. Broadcasting in any ad hoc network is an elementary operation required for the core system functionality. However, intentional broadcasting by flooding may introduce uncontrollable redundancy, contention, and collisions that would lead to a so-called broadcast storm problem.

The rest of this work is organized as follows. Section 2 introduces the proposed system model for considering a broadcast attack in the network of interest. Further, in Sect. 3 we prototype the corresponding ad hoc WSN deployment and attack it by following said approach. In Sect. 4, we propose a simple analytical model validating our proposed framework. Finally, the conclusions are drawn in the last section.

2 Considered WSN System Model

In this work, we consider a system hosting a number of autonomous wireless nodes equipped with a set of measuring modules (sensors), and thus the challenges of efficient data transmission and processing are brought into focus [20]. On the other hand, ad hoc WSNs of this type are susceptible to possible attacks by implosion, blind flooding and, finally, broadcast storm [21–23].

Focusing primarily on the most challenging broadcast storm concept, the multicast control messages in a mission-critical WSN may become the main vehicles of this attack. Therefore, a high number of such packets is affecting the QoS for each transmitting node, which results in shorter battery life and lower reliability. The main configuration flaws that may enable such an attack are listed in what follows:

1. No limitations on the packet time-to-live parameter;
2. A possibility to transmit a broadcast packet from any unknown address in the network;
3. A device that could continuously generate packets.

Our research indicates that the easiest and cheapest way for an attacker to affect the operation of the ad hoc network in question is to generate harmful messages, when already residing *inside* the network. This may cause not only a partial denial-of-service effect for one particular node, but also provoke a fault of the entire wireless network [24]. Another factor affecting the system operation with substantial impact is a lack of continuous management and support, i.e. the network is assumed to be a standalone instance without continuous monitoring exercised. Some of the devices may become disabled due to natural factors, and may not be replaced immediately. However, there should always remain a crucial number of the operational devices available to deliver an alarm message. Summarizing all of the above, in this paper we focus on the problem of probabilistic device availability estimation in cases of a broadcast storm attack.

The most common implementation of said attack may be described as a significant increase in the intensity of broadcast requests in the target WSN or flooding by the attacker device, as it is presented in Fig. 2. As each transceiver

node has to rebroadcast the messages, it leads to the difficulties in serving them over the reliable time. Basically, this scenario would appear when the incoming buffer of the device is full and/or the wireless channel is congested [25], and thus the denial-of-service attack is successful [26].

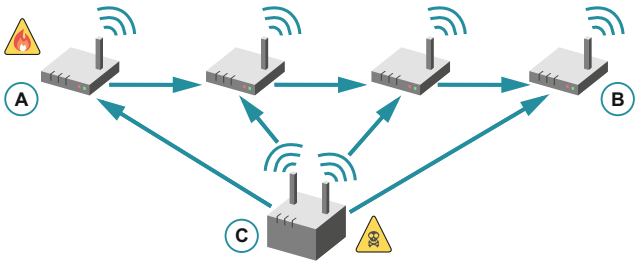


Fig. 2. Implementing the broadcast storm attack in an ad hoc WSN

In our target scenario, we employ the widely used WSN technology, IEEE 802.15.4 (ZigBee) [27], under the broadcast storm conditions. The WSN nodes equipped with such a radio module are typically small autonomous devices with limited computational power [28]. They are operating under a predefined configuration and utilize a constant set of vendor-specific signaling messages.

3 Prototyping a Broadcast Storm Attack

In order to verify the feasibility of our above discussion, we have conducted a set of experimental tests utilizing ZigBee-equipped Telegesis ETRX357 devices [29]. The prototype structure is given in Fig. 2 and the actual deployment example is presented in Fig. 3. Here, the traffic is transmitted from the device A to the device B via the relying node. USB-dongle C is utilized as the attacker device, generating broadcast messages.

The main goal of our installation is to obtain the probabilistic packet loss values. We assume a high-density industrial WSN deployment, where each node may receive data not only from its immediate neighbor, but also from the attacker device, thus escalating the effects of the broadcast storm. Node B as the destination device analyzes the amount of received meaningful data as well as the share of unclassified (attacker's) packets. The key setup parameters and the corresponding notation are given in Table 1.

Further, we analyze the impact produced by the attacker on the packet transmission delay, and the respective results are presented in Fig. 4(a) and (b). For our test scenario, we utilize two Telegesis command types (i) AT+N and (ii) AT+SN:00 [30]. The first command has as its main purpose to request the node's surrounding network information. The second command AT+SN is generally used to force a particular device to scan the network and "00" causes each

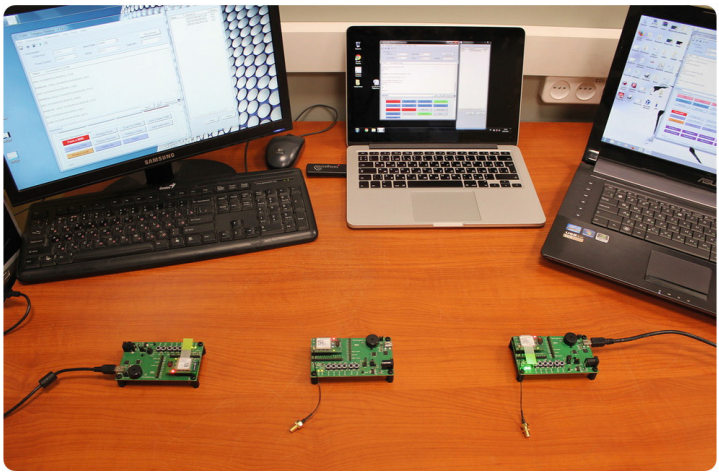


Fig. 3. Photo of the practical test deployment

Table 1. Main setup parameters

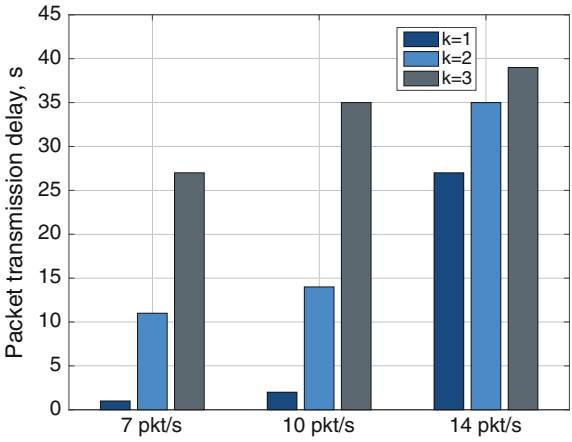
Parameter	Description	Practical value
λ_p	Packet arrival rate	120 packets per second
λ_{sh}	Attacker's packet arrival rate	1–15 packets per second
μ	Packet service rate	180 packets per second
n	Buffer size	10 packets
k	Number of relaying nodes	1, 2, 3
n	Packet size	15 kb
T	System throughput	250 kbps

attacked node to search across the entire network for neighbors. As we learn from the test results, by increasing the packet arrival rate one might cause a dramatic surge in the delay for up to 2 times by only introducing 14 additional broadcast messages in our network. Importantly, this extra packet delay has a direct impact on the energy consumption values due to increased packet retransmission cost after a collision in the wireless channel.

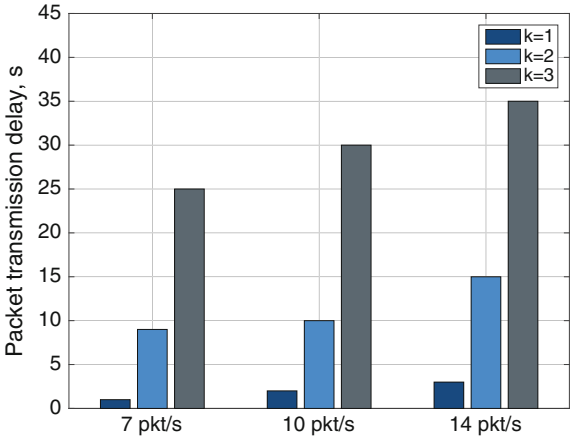
We emphasize the fact that prototyping of a large-scale real-world WSN is difficult to implement in the laboratory environment due to the space limitations and thus we decided to support our test deployment with a simple analytical model that can validate and predict the ad hoc WSN behavior under broadcast storm conditions.

4 Supportive Analytical Modeling of Our Prototype

By employing simple methods of the queuing theory in our model [31], we first assume that the packet loss probability is not affected by the attacker. We further



(a) Broadcast packet type: AT+N



(b) Broadcast packet type: AT+SN:00

Fig. 4. Data transmission delay based on attacker's packet arrival rate (prototype)

consider that the packet generation intensity on the end-device is given as a Poisson process and that the packet service interval is distributed exponentially [32]. We verify this hypothesis at the end of this work. Hence, in the single-relay WSN case the packet loss probability may be calculated as

$$P_l = \rho^n \frac{1-\rho}{1-\rho^{n+1}}, \quad \rho = \frac{\lambda}{\mu}, \tag{1}$$

where λ is the packet arrival rate, μ is the packet service rate, and n is a node's buffer size.

Further, for the multi-relay case we modify Eq. (1) accordingly

$$P_l^k = 1 - (\rho^n \frac{1-\rho}{1-\rho^{n+1}})^k, \tag{2}$$

where k is the number of relaying hops.

The majority of the analytical frameworks available today do not take into account the attacker [33–36] that can initiate an attack by generating the broadcast messages with higher arrival rate.

Every broadcast packet is served by each attacked WSN node and then forwarded to the following hop. Clearly, the number of nodes under attack could be significantly increased if the attacker would modify the radio equipment to utilize transmission at higher power.

Further, using Eqs. (1) and (2), we evaluate the packet loss probability for a network affected by the broadcast storm attack as follows

$$\begin{cases} P_l^{k=1} = 1 - \left(1 - \left(\frac{\lambda_p + \lambda_{sh}}{\mu}\right)^n \frac{1 - \left(\frac{\lambda_p+\lambda_{sh}}{\mu}\right)}{1 - \left(\frac{\lambda_p+\lambda_{sh}}{\mu}\right)^{n+1}}\right), k = 1 \\ P_l^{k\geq 2} = P_l^{k=1} \prod_{k=2}^{m} \left(1 - \left(\frac{\lambda_p + k\lambda_{sh}}{\mu}\right)^n \frac{1 - \left(\frac{\lambda_p+k\lambda_{sh}}{\mu}\right)}{1 - \left(\frac{\lambda_p+k\lambda_{sh}}{\mu}\right)^{n+1}}\right), k \geq 2 \end{cases} \tag{3}$$

where λ_{sh} is the attacker packet arrival rate.

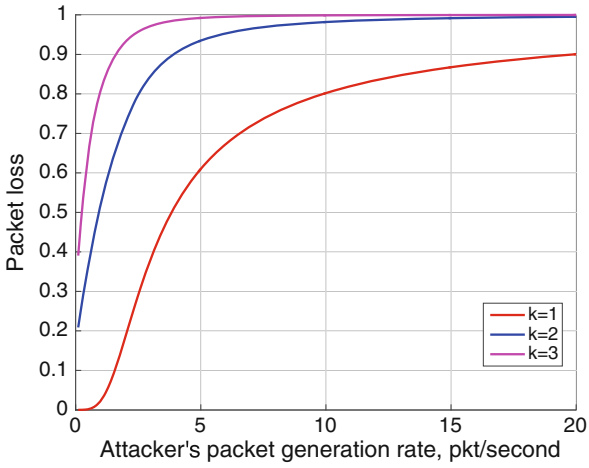
In order to quantitatively characterize the proposed prototype, we first study the impact of the system parameters on the packet loss rates. To this end, Fig. 5(a) shows the influence of the attacker's packet generation rate on the WSN packet loss at a fixed WSN node data generation rate. Clearly, by increasing the number of affected relaying nodes system saturation is achieved faster. This is due to the broadcast message distribution, which has repetitive nature.

In our second scenario presented in Fig. 5(b), we fix the attacker's packet generation rate and vary that of the WSN node. As we observe in the plots, the ad hoc network is providing a certain level of QoS even in the situation when the node's packet generation rate is higher than the service rate.

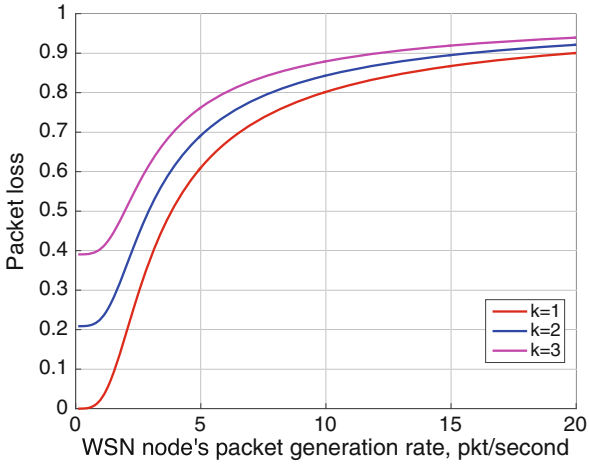
Our third scenario depicted in Fig. 6 corresponds to a situation, when both node's and attacker's packet generation rates are fixed and only the service rate is varied. Accordingly, for each number of relaying nodes we can find the corresponding lowest service rate to guarantee the minimal reachable packet loss for a particular attacker's packet generation rate.

Furthermore, our simple analytical model is able to probabilistically predict the likely ad hoc WSN conditions taking into account the effects of the broadcast storm attack that alters the underlying packet generation rate.

Finally, we compare the analytical and prototype packet loss performance based on the key system parameters given in Table 1. By focusing on the obtained prototype-driven results and those delivered by our analytical prediction, as summarized in Fig. 7, it can be concluded that the analytical and the experimental values agree within acceptable bounds.



(a) Attacker traffic



(b) Node traffic

Fig. 5. Impact of packet generation rate on packet loss rate

To confirm the obtained results, we have additionally verified our prototype-based and analytical data using Pearson's chi-squared test [37] with $\alpha = 0.05$ by executing a set of 100 independent trials. Therefore, it could be concluded that the resulting difference between the compared distributions of the packet loss values in a realistic WSN under the broadcast storm conditions is statistically insignificant. Thereby, our initial assumption on the Poission packet arrival distribution and the exponential service time distribution are practical.

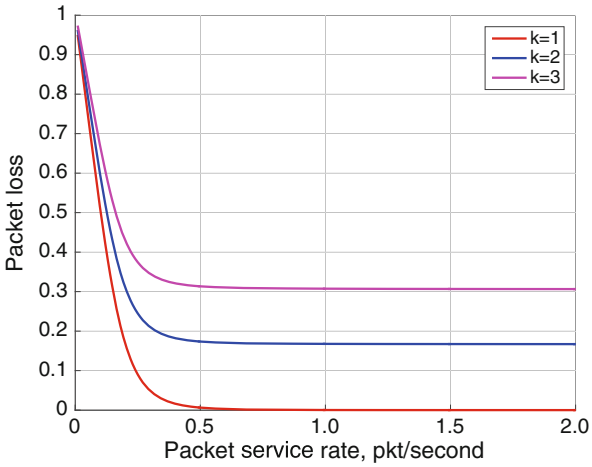


Fig. 6. Impact of packet service rate on the system packet loss rate under broadcast storm attack $\lambda_p = \lambda_{sh}$

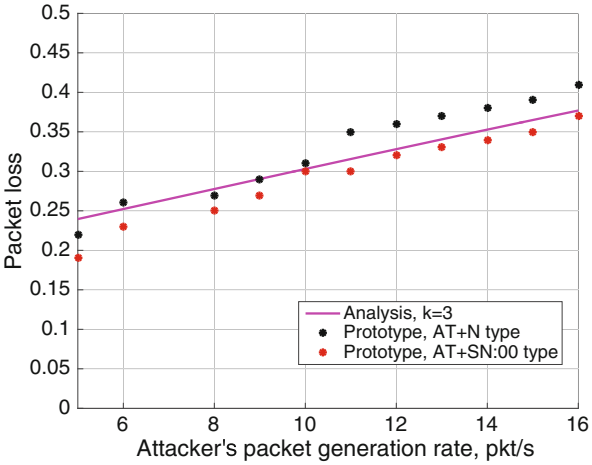


Fig. 7. Analytical results agreeing with our experimental setup

5 Conclusions

This paper developed a model and the respective practical prototype of a broadcast storm attack, which may disrupt the desired reliable operation of a mission-critical WSN deployment. To this end, we collected the packet loss probabilities together with the packet transmission delays produced with our testbed, and compared some of those against the corresponding values provided with our simple queuing theoretic model. The obtained results not only evidence the feasibility of this convenient custom-made approximation for predicting the operational

parameters of a real-world WSN under attack, but also help identify conditions that become threatening for the intended operation of the industrial monitoring system under consideration.

References

1. Iyengar, S.S., Brooks, R.R.: Distributed Sensor Networks: Sensor Networking and Applications. CRC Press, Boca Raton (2012)
2. Hendee, J., Gramer, L., Heron, S., Jankulak, M., Amornthammarong, N., Shoemaker, M., Burgess, T., Fajans, J., Bainbridge, S., Skirving, W.: Wireless architectures for coral reef environmental monitoring. In: Proceedings of the 12th International Coral Reef Symposium, Cairns, Australia (2012)
3. Vinel, A., Vishnevsky, V., Koucheryavy, Y.: A simple analytical model for the periodic broadcasting in vehicular ad-hoc networks. In: Proceedings of the GLOBECOM Workshops, pp. 1–5. IEEE (2008)
4. Aslan, Y.E., Korpeoglu, I., Ulusoy, Ö.: A framework for use of wireless sensor networks in forest fire detection and monitoring. Comput. Environ. Urban Syst. **36**(6), 614–625 (2012)
5. Dohler, M., Vilajosana, I., Vilajosana, X., LLosa, J.: Smart cities: An action plan. In: Proceedings of the Barcelona Smart Cities Congress (2011)
6. Andreev, S., Gonchukov, P., Himayat, N., Koucheryavy, Y., Turlikov, A.: Energy efficient communications for future broadband cellular networks. Comput. Commun. **35**(14), 1662–1671 (2012)
7. Rashid, B., Rehmani, M.H.: Applications of wireless sensor networks for urban areas: a survey. J. Netw. Comput. Appl. **60**, 192–219 (2016). Elsevier
8. Kim, S., Pakzad, S., Culler, D., Demmel, J., Fenves, G., Glaser, S., Turon, M.: Health monitoring of civil infrastructures using wireless sensor networks. In: Proceedings of the 6th International Symposium on Information Processing in Sensor Networks (IPSN), pp. 254–263. IEEE (2007)
9. Pakzad, S.N., Kim, S., Fenves, G.L., Glaser, S.D., Culler, D.E., Demmel, J.W.: Multi-purpose wireless accelerometers for civil infrastructure monitoring. In: Proceedings of the 5th International Workshop on Structural Health Monitoring (IWSHM) (2005)
10. Kumar, P., Ylianttila, M., Gurtov, A., Lee, S.-G., Lee, H.-J.: An efficient and adaptive mutual authentication framework for heterogeneous wireless sensor network-based applications. Sensors **14**(2), 2732–2755 (2014)
11. Sridhar, P., Sheikh-Bahaei, S., Xia, S., Jamshidi, M.: Multi-agent simulation using discrete event and soft-computing methodologies. In: Proceedings of the International Conference on Systems, Man and Cybernetics, vol. 2, pp. 1711–1716. IEEE (2003)
12. Wright, J.: Killerbee: practical ZigBee exploitation framework. In: Proceedings of the 11th ToorCon Conference, San Diego (2009)
13. Chen, Y., Xu, W., Trappe, W., Zhang, Y.: Detecting and localizing wireless spoofing attacks. In: Securing Emerging Wireless Systems, pp. 1–18. Springer, New York (2009)
14. Patwari, N., Hero III, A.O., Perkins, M., Correal, N.S., O'dea, R.J.: Relative location estimation in wireless sensor networks. IEEE Trans. Signal Process. **51**(8), 2137–2148 (2003)

15. Hosek, J., Masek, P., Kovac, D., Ries, M., Kropfl, F.: Universal smart energy communication platform. In: Proceedings of the International Conference on Intelligent Green Building and Smart Grid (IGBSG), pp. 1–4. IEEE (2014)
16. Conti, M., Giordano, S.: Mobile ad hoc networking: milestones, challenges, and new research directions. IEEE Commun. Mag. **52**(1), 85–96 (2014)
17. Page, J., Zaslavsky, A., Indrawan, M.: Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities. In: Proceedings of the First International Workshop on Safety and Security in Multi-Agent Systems (SASEMAS 2004), pp. 85–101 (2004)
18. Zikratov, I.A., Lebedev, I.S., Gurtov, A.V.: Trust and reputation mechanisms for multi-agent robotic systems. In: Balandin, S., Andreev, S., Koucheryavy, Y. (eds.) NEW2AN/ruSMART 2014. LNCS, vol. 8638, pp. 106–120. Springer, Heidelberg (2014)
19. Tseng, Y.-C., Ni, S.-Y., Shih, E.-Y.: Adaptive approaches to relieving broadcast storms in a wireless multihop mobile ad hoc network. IEEE Trans. Comput. **52**(5), 545–557 (2003)
20. Wyglinski, A.M., Huang, X., Padir, T., Lai, L., Eisenbarth, T.R., Venkatasubramanian, K.: Security of autonomous systems employing embedded computing and sensors. Micro, IEEE **33**(1), 80–86 (2013)
21. Lipman, J., Liu, H., Stojmenovic, I.: "Broadcast in ad hoc networks," in Guide to wireless ad hoc networks, pp. 121–150, Springer, (2009)
22. Hu, Y.-C., Perrig, A., Johnson, D.B.: Rushing attacks and defense in wireless ad hoc network routing protocols. In: Proceedings of the 2nd ACM Workshop on Wireless Security, pp. 30–40. ACM (2003)
23. Tseng, Y.-C., Ni, S.-Y., Chen, Y.-S., Sheu, J.-P.: The broadcast storm problem in a mobile ad hoc network. Wireless Netw. **8**(2–3), 153–167 (2002)
24. Korzun, D.G., Nikolaevskiy, I., Gurtov, A.: Service intelligence support for medical sensor networks in personalized mobile health systems. In: Balandin, S., Andreev, S., Koucheryavy, Y. (eds.) NEW2AN/ruSMART 2015. LNCS, vol. 9247, pp. 116–127. Springer, Heidelberg (2015)
25. Kelly IV., C., Ekanayake, V., Manohar, R.: SNAP: A sensor-network asynchronous processor. In: Proceedings of the 9th International Symposium on Asynchronous Circuits and Systems, pp. 24–33. IEEE (2003)
26. Denko, M.K.: Detection and prevention of denial of service (dos) attacks in mobile ad hoc networks using reputation-based incentive scheme. J. Systemics, Cybern. Inf. **3**(4), 1–9 (2005)
27. Xu, S., Man, Y., He, H., Zhao, L., Zheng, Y., Wang, T.: A security personnel information collection system based on ZigBee wireless ad-hoc network. In: Proceedings of the International Conference on Computer and Communications (ICCC), pp. 410–414. IEEE (2015)
28. Andreev, S., Koucheryavy, Y., Himayat, N., Gonchukov, P., Turlikov, A.: Active-mode power optimization in OFDMA-based wireless networks. In: Proceedings of the GLOBECOM Workshops, pp. 799–803. IEEE (2010)
29. Telegesis, The ETRX357-DVK development kit is an ideal starting point for development and evaluation of the ETRX357 2.4 GHz ZigBee modules, February 2016. http://www.telegesis.com/products/etrx3-based-products/etrx3-zigbee-development-kit/
30. Telegesis, ETRX2 and ETRX3 Series ZigBee Modules AT-Command Dictionary, December 2014. http://www.telegesis.com/download/document-centre/etrx3_technical_manuals/TG-ETRXn-R308-Commands.pdf

31. Bisnik, N., Abouzeid, A.A.: Queuing network models for delay analysis of multihop wireless ad hoc networks. Ad Hoc Netw. **7**(1), 79–97 (2009)
32. Andreev, S., Galinina, O., Koucheryavy, Y.: Energy-efficient client relay scheme for machine-to-machine communication. In: Proceedings of the Global Telecommunications Conference (GLOBECOM 2011), pp. 1–5. IEEE (2011)
33. Zhao, J., Govindan, R., Estrin, D.: Computing aggregates for monitoring wireless sensor networks. In: Proceedings of the First International Workshop on Sensor Network Protocols and Applications, pp. 139–148. IEEE (2003)
34. Ni, Y., Ye, X., Ko, J.: Monitoring-based fatigue reliability assessment of steel bridges: analytical model and application. J. Struct. Eng. **136**(12), 1563–1573 (2010)
35. Moltchanov, D., Koucheryavy, Y., Harju, J.: Simple, accurate and computationally efficient wireless channel modeling algorithm. In: Braun, T., Carle, G., Koucheryavy, Y., Tsaoussidis, V. (eds.) WWIC 2005. LNCS, vol. 3510, pp. 234–245. Springer, Heidelberg (2005)
36. Li, Z., Chan, T.H., Ko, J.M.: Fatigue analysis and life prediction of bridges with structural health monitoring data–part i: methodology and strategy. Int. J. Fatigue **23**(1), 45–53 (2001)
37. Pearson, K.: X. on the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. London, Edinb., Dublin Philos. Mag. J. Sci. **50**(302), 157–175 (1900)