Challenges of Misbehavior Detection in Industrial Wireless Networks

Sebastian Henningsen, Stefan Dietzel, Björn Scheuermann

Humboldt-Universität zu Berlin, Berlin, Germany
sebastian.henningsen@hu-berlin.de, stefan.dietzel@hu-berlin.de,
scheuermann@informatik.hu-berlin.de

Abstract. In recent years, wireless technologies are increasingly adopted in many application domains that were either unconnected before or exclusively used cable networks. This paradigm shift towards – often ad-hoc – wireless communication has led to significant benefits in terms of flexibility and mobility. Alongside with these benefits, however, arise new attack vectors, which cannot be mitigated by traditional security measures. Hence, mechanisms that are orthogonal to cryptographic security techniques are necessary in order to detect adversaries. In traditional networks, such mechanisms are subsumed under the term "intrusion detection system," and many proposals have been implemented for different application domains. More recently, the term "misbehavior detection" has been coined to encompass detection mechanisms especially for attacks in wireless networks. In this paper, we use industrial wireless networks as an exemplary application domain to discuss new directions and future challenges in detecting insider attacks. To that end, we review existing work on intrusion detection in mobile ad-hoc networks. We focus on physical-layer-based detection mechanisms as these are a particularly interesting research direction that had not been reasonable before widespread use of wireless technology.

Key words: physical-layer security, wireless security, industrial wireless networks, intrusion detection

1 Introduction

Cyber-physical systems, such as, power plants, intelligent transportation systems, connected cars, or industrial automation systems, were traditionally mostly autonomous. As their connectivity increases, a constant threat arises by both insider and outsider adversaries with varying motivations. One source of motivation is industrial espionage, where a competitor tries to obtain secret intellectual property in order to void a technological advantage. Also, acts of sabotage in the name of national security have been observed. Famously, the Stuxnet virus [1] presumably targeted nuclear facilities in Iran. Attacks on cyber-

S. Henningsen et al., "Challenges of Misbehavior Detection in Industrial Wireless Networks" in *Ad Hoc Networks*, Y. Zhou and T. Kunz (Eds.). 2018
The final publication is available at Springer via https://link.springer.com/chapter/10.1007/978-3-319-74439-1_4

physical systems may lead to severe disadvantages for companies, and they may even endanger lives.

Importantly, most attacks on industrial communication are mounted from within the network. As recent attack examples demonstrate, adversaries often infiltrate their target systems and then act as insiders, using compromised systems within the network's trusted perimeter. Therefore, additional layers of defense are necessary when cryptographic protection, like encryption and signatures, are compromised. Mechanisms are required that inspect messages and message sequences in order to ensure their plausibility and consistency. These mechanisms are usually subsumed under the term Intrusion Detection System (IDS). In industrial networks, such systems are important to detect active insider attacks. As existing general-purpose IDS cannot simply be converted for use in industrial settings, researchers have made tailored proposals that include application semantics (e. g., [2]–[4]). These proposals typically apply to wired industrial communication architectures, such as the supervisory control and data acquisition (SCADA) system.

Whereas these example attacks and tailored IDS target traditional IT infrastructure that is mostly wired, recent advances in wireless technology have led to a pervasive adoption of wireless systems – including their use for industrial communication. Depending on the use case, the industrial communication networks' structure differs widely between closed-loop systems and ad-hoc topologies. Common to all applications are tight resource constraints, for example, on the latency or expected throughput.

Fundamentally, the shift towards wireless connectivity opens up new attack vectors due to the wireless medium's broadcast nature. Eavesdropping and jamming of packets, for instance, are simplified significantly. Moreover, with increased flexibility, industrial communication systems become more complex and require more maintenance. This additional maintenance extends the risk of inside adversaries, such as disguised IT-maintenance personnel. To counteract these novel attack forms, the term "misbehavior detection" emerged, which can be seen as a subform of IDS for wireless systems [5]–[7]. Example mechanisms for misbehavior detection are two-step ACKs [8], monitoring watchdogs [9] and automatic feature correlation [10]. These approaches, however, may not always be suited for particular situations. For example, due to resource constraints, misbehavior detection in industrial wireless communication systems is challenging and closely related to existing approaches for mobile ad-hoc networks (MANETs). Instead, lightweight misbehavior detection based on physical-layer characteristics can be used. These physical-layer characteristics depend on the sender's location and are, in contrast to the communication's content, not spoofable by an adversary. Misbehavior detection mechanisms can leverage these channel characteristics for adversary detection – a practice located in the field of physical-layer security. In particular, lightweight security based on physical-layer properties is well-suited for this task.

Therefore, in this paper, we discuss the potential and challenges of misbehavior detection mechanisms in industrial wireless communication. We elaborate

on these challenges (Section 2) before turning to existing approaches for attack detection algorithms in MANETs in Section 3. In particular, we state their assumptions and limitations and discuss whether ideas can be transferred industrial wireless use cases. We identify the challenge of trusted information dissemination in multi-hop networks with potential adversaries, which we investigate in Section 4 alongside with suggestions for possible solutions. We summarize pointers for future research and conclude the paper in Section 5.

2 Challenges of industrial misbehavior detection

Due to new attack vectors, the development of misbehavior detection frameworks for emerging industrial networks is important to add an additional layer of security to these systems. Traditional wired industrial automation systems and emerging – more general and flexible – wireless systems are fundamentally different. Therefore, existing IDS techniques cannot easily be transferred to the new use case, necessitating novel mechanisms.

Challenges arise due to the variety of different application scenarios and industrial wireless networks' contradictory requirements. On the one hand, use cases in industrial wireless networks range from closed-loop systems with low latency and low packet error rate, to multi-hop information propagation from sensors to data sinks. These applications differ not only in their respective scenario but also in requirements and communication characteristics. In closed-loop systems, for example, communication is synchronized and optimized for maximum throughput and minimal packet error rate, while not providing flexibility in terms of joining/parting nodes. Multi-hop information propagation, as the other extreme, is flexible in the topology and can easily tolerate packet errors but cannot achieve minimal delay. Hence, the challenge when developing misbehavior detection techniques is to not only cope with these differences but rather leverage these characteristics. Domain-specific properties should be used to develop tailored mechanisms for each use case in order to achieve maximal detection performance and security. On the other hand, contradictory requirements regarding the properties of industrial wireless networks lead to additional challenges in the design of misbehavior detection systems. Closed-loop, low-latency wireless networks, for example, aim at achieving wire-equivalent performance while providing more security than traditional wire-based systems. Hence, the security mechanisms must be as lightweight as possible but still maintain a high security standard – a tradeoff that has to be accounted for in the development of suitable misbehavior detection approaches. Thus, the challenge when designing these approaches lies in this tradeoff and finding the equilibrium between performance and security.

Therefore, lightweight misbehavior detection systems are necessary, which inflict as little resource usage as possible while still maintaining a sufficient level of security. Particularly promising approaches for this task are passive physical-layer security mechanisms, which monitor the communication and only send messages in the presence of suspicious activities. The resource-friendly availability

of these channel measurements makes them well suited for resource-constrained networks, such as, industrial automation systems or MANETs. Passive physical-layer security has been employed for misbehavior detection in MANETs, especially for Sybil attack detection [11]–[13] and classical intrusion detection [14], [15]. Two questions arise: can these techniques be transferred from MANETs to industrial communication systems? And, what are the potential limitations and future research directions?

3 New challenges – old solutions?

In the following, we discuss existing physical-layer approaches for MANETs and their applicability to industrial wireless networks. Physical-layer security leverages physical properties to enhance security, which involves diverse topics such as distance bounding [16], key derivation [17], node authentication [18], and intrusion detection [19]. We distinguish between active and passive mechanisms: active physical-layer security algorithms require additional actions, such as, a challenge-response communication in distance bounding. Passive mechanisms, in contrast, simply monitor the desired physical properties of the communication channel between the monitoring node and the sender. The channel between sender and receiver determines how wireless signals are altered by the environment through, for instance, reflections and diffractions. Due to these environmental effects, each location is unique in terms of how the signal arrives at the receiver [20]. Moreover, the pairwise channel between sender and receiver cannot be estimated through eavesdropping at different locations and is, therefore, considered a shared secret [17]. The channel properties are estimated by the receiver at the beginning of each transmission sequence; hence, these measurements are readily available without inducing additional network load – a significant advantage over traditional cryptographic methods.

The applicability of some existing works is hindered by strong assumptions on the attacker or the network in general. Newsome *et al.* [12], for example, propose a radio resources testing scheme based on dividing the frequency band into subchannels for each neighbor. Under the assumption that the attacker radio can only listen and send on a single frequency, Sybil nodes will be detected. Besides the limitation in network bandwidth, an attacker may use multiple antennas to circumvent this mechanism. Similarly, in [21], [22], a low-mobility network is assumed, which is not generally the case for industrial communication systems.

In their seminal work, Demirbas *et al.* [23] propose a detection mechanism based on Received Signal Strength Indicator (RSSI) measurements. Their work is an implementation of [24], where a framework of four collaborating honest nodes is used to locate a node. It is proven that no node can hide its position when monitored by four honest nodes. The authors point out that exactly locating a node is not necessary in order to detect Sybil attacks; instead, it suffices to process the measured RSSI values directly. The approach is applicable in general scenarios, though in both works, the problem of information dissemination and selection of honest nodes is not tackled.

Sybil detection using RSSI measurements has subsequently been adopted in a number of works [21], [22], [25], [26]. These approaches, however, are based on strong assumptions regarding the mobility in the network or the attacker's capabilities. In [22], for example, it is assumed that the attacker cannot control transmission power, whereas Wang *et al.* [25] assume no mobility in the network. Although Wang *et al.*'s assumptions do not hold in industrial communication systems, the proposed hierarchical approach to Sybil detection is insightful and can be easily transferred to other application domains. Information is shared by flooding, which is robust but suffers from low performance.

An analytical justification of Sybil detection via channel measurements is given by Xiao *et al.* [20], who theoretically analyze the Channel Impulse Response (CIR). It is shown that the CIR quickly de-correlates with distance. Based on this theoretical analysis, a hypothesis test – Sybil attacker present or not – is proposed. The necessary parameters for this hypothesis test are derived from the theoretical model. Chen *et al.* [27], [28] extend this theoretical treatment to Received Signal Strength. The conducted analysis provides valuable insights not only for MANETs but also for other application domains. The attacker detection in [18], [20], [29], [30] is based on hypothesis testing of only the last measurement, which may not be enough if large channel fluctuations occur. Subsequent works are based on a k-means cluster analysis by maintaining a sliding window of past measurements, which is more suitable for the industrial use case. Again, when measurements from multiple nodes are combined, the focus lies on the detection algorithm rather than information dissemination.

The field of secure localization is also closely related to the detection of Sybil attacks, since an attacker cannot forge multiple fake identities if each network node can be localized. Localization techniques that were not designed with an adversarial setting in mind, however, suffer shortcomings and potential security weaknesses in the presence of an attacker [31], [32]. Hence, secure localization approaches can either cope with attacker-injected outliers [33] or use unforgeable physical properties to make attacks impossible [32]. Thwarting attacks by making algorithms more robust is a promising idea but a difficult task and requires careful consideration of the use case and attacker model at hand, thus providing interesting research challenges. In general, since secure localization schemes are oftentimes based on active measurements [32], [34], they are not particularly well suited for enhancing the security in industrial wireless networks.

Passive physical-layer techniques based on channel properties are not only employed for Sybil detection, but also for misbehavior detection in general. In fact, in an IDS, the detection of Sybil attacks and impersonation attacks is one of many monitoring tasks. In these wireless intrusion detection systems, passive physical-layer security techniques are used as one possible source of information [14], [15]. A key observation of wireless intrusion detection systems is that a single metric is not enough for adequate attacker detection. When detecting jammers, for example, Xu *et al.* have shown that with a single metric, such as RSSI, not all potential jamming strategies can be detected [35], [36]. Instead, the authors propose a combination of different indicators, such as RSSI, packet

delivery ratio, and node location, to detect and mitigate jamming attacks. The combination significantly improves the detection performance, an observation that applies to other use cases, as well [9], [32], [37]. Hence, relying on a single metric for intrusion detection is not enough, instead one has to take into account all available information.

4 New solutions are necessary

As we have seen, a number of channel-based physical-layer security approaches for MANETs exist. Most of these ideas require additional research to transform existing knowledge into misbehavior detection techniques in industrial wireless networks. A promising general idea is to leverage the wireless medium's broadcast nature by aggregating data from multiple nodes for improved detection accuracy. Common to all algorithms that rely on multiple cooperating nodes or distributed measurements is the challenge of information dissemination. Especially in an adversarial setting, trusted communication among the monitoring nodes is a vital aspect of these algorithms.

Depending on the attacker model, this problem may be easily solvable with traditional cryptographic mechanisms. If we, however, assume an inside attacker with access to key material, as motivated in Section 1, authenticity and integrity cannot be guaranteed anymore. Attackers could easily jam the communication of an honest node [38] and inject their own data instead. These challenges have been investigated separately in great detail and suitable solutions have been proposed for the individual aspects: cryptographic mechanisms at least ensure authenticity as well as integrity, jamming can be detected in many cases [35], and cloned/overtaken nodes can be detected [39], [40]. However, individual solutions assume different attacker models and thus can not necessarily be combined.

In the end, given an attacker with the ability to inject/jam packets, distributed information sharing is closely related to the notion of trust. Trust can be node-centric or data-centric, i.e., to which degree the bearer of information is trusted and how plausible the data is. Especially in multi-hop networks in the presence of an attacker, the trust in a certain data item quickly decreases in the number of hops between sender and receiver. In particular, the trust in received information depends on both, the data itself, as well as the nodes traversed on the routing path. When designing distributed algorithms, these complex trust relationships should therefore explicitly be taken into account in order to make the system more resilient against attacks.

While the notion of trust is intuitive to most, several questions arise in the context of communication networks: How to quantify and compute trust? How to include trust into, e.g., routing and attacker detection decisions? How to deal with inconsistent "trust views" or opinions between the nodes? Most Sybil attack detection algorithms are based on statistical methods, such as hypothesis testing [18], [20], [29], [30] or machine learning algorithms [27]. Hence, their output is not binary but probabilistic. Although this output could serve as the basis

for trust derivation, it is not trivial to cope with statistical outliers nor to normalize the resulting values. Optimally, the trust should depend on the situation rather than the underlying algorithm; thus, some sort of output normalization is necessary. Additionally, the data should contribute to the trust computation as well. Hence, every node must have some model, theoretical or empirical, for each neighbor, specifying the expected range of data. Since the nodes are often resource constrained, one has to face a tradeoff between accuracy and cost of these models. Moreover, the transitive computation of trust over multiple hops is a difficult challenge. If a node does not trust a direct neighbor, any information transferred via that neighbor is questionable. One is tempted to simply dismiss these transitive relationships and focus on the direct neighbors instead, which would, however, give an attacker an easy leverage to disturb the network. Last but not least, computing trust for more than just immediate neighbors is a difficult task: one has to design suitable metrics and is still facing the problem of obtaining reliable information on multi-hop neighbors.

Including computed trust values into routing and attacker detection decisions poses another challenge. When incorporating data from multiple sources in distributed algorithms, the trust in each particular source should influence the decision. In attack detection, for example, one could weigh each received (and missing) data item according to the computed trust associated with that packet. However, again, an attacker could exploit that mechanism to alter the decisions of the detection algorithm by decreasing the trust in honest nodes. A possible remedy is the development of robust algorithms [33], which are able to deal with or even detect intentional outliers. When every node maintains its own trust view on the network, inconsistencies can arise, which could cause difficulties when nodes are to agree on a consensus in a distributed fashion. Naturally, the trust has to be taken into account in this process. In situations without trust, this is normally achieved by Byzantine commitment protocols [41]. The combination of trust values for each packet, together with traditional Byzantine commitment protocols and the establishment of fundamental bounds on this procedure, are also a challenging research question.

A potential method to formally capture trust relationships in general is subjective logic [42]. Subjective logic is a powerful and flexible framework for reasoning under uncertainty, in which facts or measurements are extended to opinions in order to incorporate said uncertainty. It provides notions for data-centric trust and node-centric trust, as well as operators to combine opinions, which can be used to model trust relationships. In particular, subjective logic provides several operators in order to reduce trust chains to a single logical opinion. The choice of operators depends on the setting at hand and requires careful consideration.

5 Concluding outlook on future research

In this paper we discussed the challenges of misbehavior detection in industrial wireless networks. These challenges arise in multiple aspects, from jamming detection and prevention to malicious packet injection; hence, a holistic perspective

is required to design suitable solutions. Although it is reasonable to focus on a particular aspect in research, a heterogeneous landscape of different assumptions and models makes it difficult to combine individual ideas. We believe that a harmonization of models is necessary so that the design of a complex systems from individual parts is facilitated.

As we have seen in Section 3, physical-layer information, which is readily available without any additional cost, has been successfully leveraged for attacker detection. Due to firmware constraints in commercial off-the-shelf hardware, often only coarse-grained information, such as RSSI, is reported to higher layers. However, more fine-grained CIR information is available, which would significantly increase the performance of detection algorithms [43]. Thus, in our view, the development of suitable firmwares capable of providing more information is an important step towards future solutions.

Last but not least, we discussed information dissemination in adversarial multi-hop environments. We propose to include the notion of trust into algorithms and protocols in order to dependably spread information. Possible directions for future research include (1) the computation of the trust itself, especially over multiple hops, (2) the incorporation of trust into existing protocols, and (3) trust-based distributed consensus.

Acknowledgments

The work was partly funded by the German Federal Ministry of Education and Research under BMBF grant agreement no. 16KIS0222.

References

[1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, 2011.

[2] D. Hadžiosmanović, R. Sommer, E. Zambon, *et al.*, "Through the eye of the plc: Semantic security monitoring for industrial processes," in *Proc. of the 30th Annual Computer Security Applications Conference*, ser. ACSAC, ACM, 2014.

[3] D. Hadziosmanovic, D. Bolzoni, S. Etalle, *et al.*, "Challenges and opportunities in securing industrial control systems," in *2012 Complexity in Engineering (COMPENG). Proceedings*, Jun. 2012.

[4] F. Kargl, R. W. van der Heijden, H. König, *et al.*, "Insights on the security and dependability of industrial control systems," *IEEE Security Privacy*, vol. 12, no. 6, Nov. 2014.

[5] S. Radosavac, J. S. Baras, and I. Koutsopoulos, "A framework for mac protocol misbehavior detection in wireless networks," in *Proceedings of the 4th ACM workshop on Wireless security*, ACM, 2005.

[6] S. Sarafijanovic and J.-Y. Le Boudec, "An artificial immune system approach with secondary response for misbehavior detection in mobile ad hoc networks," *IEEE Transactions on Neural Networks*, vol. 16, no. 5, 2005.

[7] I. Butun, S. D. Morgera, and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, 2014.

[8] K. Liu, J. Deng, P. K. Varshney, *et al.*, "An acknowledgment-based approach for the detection of routing misbehavior in manets," *IEEE transactions on mobile computing*, vol. 6, no. 5, 2007.

[9] S. Marti, T. J. Giuli, K. Lai, *et al.*, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom, ACM, 2000.

[10] Y.-a. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks," in *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, ACM, 2003.

[11] H. Yang, H. Luo, F. Ye, *et al.*, "Security in mobile ad hoc networks: Challenges and solutions," *IEEE wireless communications*, vol. 11, no. 1, 2004.

[12] J. Newsome, E. Shi, D. Song, *et al.*, "The sybil attack in sensor networks: Analysis & defenses," in *Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks*, ser. IPSN, ACM, 2004.

[13] K. Sanzgiri, B. Dahill, B. N. Levine, *et al.*, "A secure routing protocol for ad hoc networks," in *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*, IEEE, 2002.

[14] I. Onat and A. Miri, "An intrusion detection system for wireless sensor networks," in *Wireless And Mobile Computing, Networking And Communications, 2005., IEEE International Conference on*, IEEE, vol. 3, 2005.

[15] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *Journal of High Speed Networks*, vol. 15, no. 1, 2006.

[16] S. Brands and D. Chaum, "Distance-bounding protocols," in *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, ser. EUROCRYPT, Springer-Verlag New York, Inc., 1994.

[17] S. Jana, S. N. Premnath, M. Clark, *et al.*, "On the effectiveness of secret key extraction from wireless signal strength in real environments," ser. MobiCom, ACM, 2009.

[18] L. Xiao, A. Reznik, W. Trappe, *et al.*, "Phy-authentication protocol for spoofing detection in wireless networks," in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, IEEE, 2010.

[19] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proceedings of the 5th ACM workshop on Wireless security*, ACM, 2006.

[20] L. Xiao, L. J. Greenstein, N. B. Mandayam, *et al.*, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, 2008.

[21] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Signal strength based sybil attack detection in wireless ad hoc networks," in *Developments in eSystems Engineering, 2009 Second International Conference on*, IEEE, 2009.

[22] S. Abbas, M. Merabti, D. Llewellyn-Jones, *et al.*, "Lightweight sybil attack detection in manets," *IEEE systems journal*, vol. 7, no. 2, 2013.

[23] M. Demirbas and Y. Song, "An rssi-based scheme for sybil attack detection in wireless sensor networks," ser. WOWMOM, IEEE, 2006.

[24] S. Zhong, L. Li, Y. G. Liu, *et al.*, "Privacy-preserving location-based services for mobile users in wireless networks," *Department of Computer Science, Yale University, Technical Report ALEU/DCS/TR-1297*, 2004.

[25] J. Wang, G. Yang, Y. Sun, *et al.*, "Sybil attack detection based on rssi for wireless sensor network," in *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, IEEE, 2007.

[26] M. A. Jan, P. Nanda, X. He, *et al.*, "A sybil attack detection scheme for a centralized clustering-based hierarchical network," in *Trustcom/BigDataSE/ISPA, 2015 IEEE*, IEEE, vol. 1, 2015.

[27] Y. Chen, J. Yang, W. Trappe, *et al.*, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 5, 2010.

[28] Y. Chen, W. Xu, W. Trappe, *et al.*, "Detecting and localizing wireless spoofing attacks," in *Securing Emerging Wireless Systems*, Springer, 2009.

[29] L. Xiao, L. Greenstein, N. Mandayam, *et al.*, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. of ICC*, IEEE, 2008.

[30] L. Xiao, L. J. Greenstein, N. B. Mandayam, *et al.*, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, 2009.

[31] X. Du and H.-H. Chen, "Security in wireless sensor networks," *IEEE Wireless Communications*, vol. 15, no. 4, 2008.

[32] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. of the 2nd ACM Workshop on Wireless Security*, ACM, 2003.

[33] Z. Li, W. Trappe, Y. Zhang, *et al.*, "Robust statistical methods for securing wireless localization in sensor networks," in *Proc. of the 4th international symposium on Information processing in sensor networks*, IEEE, 2005.

[34] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, 2006.

[35] W. Xu, W. Trappe, Y. Zhang, *et al.*, "The feasibility of launching and detecting jamming attacks in wireless networks," ser. MobiHoc, ACM, 2005.

[36] W. Xu, K. Ma, W. Trappe, *et al.*, "Jamming sensor networks: Attack and defense strategies," *Netwrk. Mag. of Global Internetwkg.*, vol. 20, no. 3, Sep. 2006.

[37] D. Glynos, P. Kotzanikolaou, and C. Douligeris, "Preventing impersonation attacks in manet with multi-factor authentication," in *Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, 2005. Third International Symposium on*, IEEE, 2005.

[38] M. Wilhelm, I. Martinovic, J. B. Schmitt, *et al.*, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" In *Proc. of the Fourth ACM Conference on Wireless Network Security*, ser. WiSec, ACM, 2011.

[39] M. Conti, R. Di Pietro, L. Mancini, *et al.*, "Distributed detection of clone attacks in wireless sensor networks," *IEEE transactions on dependable and secure computing*, vol. 8, no. 5, 2011.

[40] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Security and Privacy, 2005 IEEE Symposium on*, IEEE, 2005.

[41] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *Trans. on Programming Languages and Systems (TOPLAS)*, vol. 4, no. 3, 1982.

[42] A. Jøsang, *Subjective Logic - A Formalism for Reasoning Under Uncertainty*, ser. Artificial Intelligence: Foundations, Theory, and Algorithms. Springer, 2016.

[43] Z. Yang, Z. Zhou, and Y. Liu, "From RSSI to CSI: Indoor localization via channel response," *ACM CSUR*, no. 2, 2013.