Extended Abstract - Transformers: Intrusion Detection Data In Disguise

James Boorman[0000−0001−9371−0789], Benjamin Green, and Daniel Prince

Lancaster University, Lancaster, United Kingdom
{j.boorman,b.green2,d.prince}@lancaster.ac.uk

Abstract. IoT cyber security deficiencies are an increasing concern for users, operators, and developers. With no immediate and holistic device-level fixes in sight, alternative wraparound defensive measures are required. Intrusion Detection Systems (IDS) present one such option, and represent an active field of research within the IoT space. IoT environments offer rich contextual and situational information from their interaction with the physical processes they control, which may be of use to such IDS. This paper uses a comprehensive analysis of the current state-of-the-art in context and situationally aware IoT IDS to define the often misunderstood concepts of context and situational awareness in relation to their use within IoT IDS. Building on this, a unified approach to transforming and exploiting such a rich additional data set is proposed to enhance the efficacy of current IDS approaches.

Keywords: Internet of Things · IoT · Intrusion Detection · Context Awareness · Situational Awareness

1 Introduction

One of the largest computing platforms in the world, the Internet of Things (IoT) is a continually evolving paradigm that aims to permeate and interconnect every facet of society. Comprised of heterogeneous devices in growing numbers sensing and interacting with each other and the surrounding world, IoT brings significant benefits to its ever expanding set of application domains.

Computationally constrained when compared to traditional computing systems, IoT devices utilise varying technologies designed to support communication using limited resources. Consequently, this exposes them to cyber attacks through their inability to adopt traditional defensive techniques [15]. These issues are compounded through deficiencies in development practices, and contribute towards IoT devices being considered as promising targets of attack [15]. This ever increasing threat necessitates the use of alternative wraparound defensive measures, including intrusion detection systems (IDS).

IDS for IoT is an active field of research, with many solutions being created to overcome device-level resource limitations [5]. However, few IDS solutions incorporate the large swathe of context and situational information generated by IoT devices. Even in micro deployments, there exists a large quantity of information

that has the potential to provide any IDS with contextual and situational understanding, empowering decision making. Authors in this space have identified the potential for context and situational awareness in IoT IDS [3]. However, the difference between these two terms is often misunderstood, with context awareness and situational awareness being mislabelled and subsequently misused [14, 22]. This presents a challenge to other researchers looking to incorporate context and situational awareness into their own IDS solutions.

In this paper we clarify the difference between context and situational awareness for IoT IDS through a comprehensive analysis of their current state-of-the-art within literature. We then offer a unified approach to generating situational awareness data for IoT IDS through a theoretical pathway, highlighting the necessary steps to take to transform raw data into situational awareness.

2 Background and Related Work

IDS for IoT is a varied and active research area, with a broad body of literature dedicated to detecting the ever increasing profile of attack techniques. While active, it is an area that faces unique challenges, with a vastly heterogeneous device base adding new concerns to long standing security issues inherited from traditional computing systems.

There exists 3 primary surveys that focus on IDS in IoT. Zarpelão et al [31] present a taxonomy to classify IDS in IoT literature, alongside a critical analysis of future research directions in this space. The authors identify that research efforts should focus on investigating detection methods and placement strategies, increasing the range of detectable attacks, addressing more IoT technologies, improving validation strategies, and overcoming the unsuitability of traditional IDS for IoT networks. Santos et al [25] provide a more recent literature review, corroborating Zarpelão et al's [31] proposed research directions, and highlight that IoT IDS is still in its infancy. Finally, Benkhelifa et al [5] critically reviewed practices and challenges in IoT IDS, before proposing an architecture supporting IoT IDS that spans all three IoT layers (perception, network, and application).

While the aforementioned surveys identify key research issues currently affecting IoT IDS, they fail to discuss or identify the use of context and situational awareness as a suitable base for augmentation. This is to be expected when considering that although there are over 900 IoT IDS papers returned from cursory searches on SCOPUS, only 24 of these are focused towards context or situational awareness for IoT IDS. Although context and situational awareness IoT IDS constitutes a very small proportion of overall IoT IDS literature, there are authors who demonstrate that context information when considered in conjunction with network information offers improvement over non-context aware IDS [3]. Furthermore, Kouicem et al's [15] survey of IoT security advocates that to improve IoT device security there should be an increased effort towards utilising the environment in which they pervade.

As demonstrated across the following sections, efforts have been made to exploit context and situational awareness within IoT IDS literature. However, there is still much confusion surrounding the difference between these two distinct terms, and how one can transform raw data into usable context and situational

awareness. Moreover, the initial attempts present in literature often claim to use context awareness, but in actuality are using situational awareness [22], and vice versa [14]. To alleviate this confusion, the following two sections outline what constitutes context and situational awareness, including the state-of-the-art for their use in IoT IDS.

3 Context and Context Awareness

3.1 Definitions

To successfully identify implementations of context awareness for IoT IDS, it is important to first understand what is meant by context and context awareness. Dey and Abowd [1], provide the following widely accepted definition of context, Definition 1, as:

"any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves"

Once understood, it becomes possible to distinguish between raw data and context information. Sanchez et al [24] posit that this distinction is simple; raw data is unprocessed and comes directly from the data source, while context information can only be generated through the processing of raw data. This distinction is important to keep in mind to ensure that the use of context information and raw data is kept separate to avoid confusion.

Following on from their definition of context, Dey and Abowd [1] provide the following widely accepted definition of context aware, Definition 2, as:

"A system is context aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task"

While both definitions are widely accepted, there are cases in which related works opt for alternative definitions [6, 16]. However, IDS for IoT using context awareness requires definitions that are generically applicable due to the heterogeneous nature of IoT devices, and where the reshaping of situations can occur from the smallest of changes in environmental composition. For this reason, Dey and Abowd's [1] definitions are preferred, as they are more generically applicable when compared with those suggested in other works.

3.2 Context and Context Awareness For IoT IDS

Before discussing context and context awareness for IoT IDS, it is first important to identify the state of context and context awareness for IoT as a whole so that an appropriate basis can be formed. Perera et al [23] provide the most comprehensive context aware IoT survey to date. In this work the authors identify factors necessary for context awareness formation, and introduce the context life cycle. This life cycle covers the movement of context in context aware systems,

and consists of four stages: Acquisition, Modelling, Reasoning, and Dissemination. Following a discussion surrounding the overall context life cycle, the authors present a number of practical techniques applicable to each stage. Sezer et al [26] build upon this to provide the most recent survey on IoT context awareness. Their work provides an overview of the state of the art in context aware IoT, and goes on to discuss new techniques supporting stages within the context life cycle, before defining context awareness as an essential part of IoT.

Anton et al [3] present a context aware intrusion detection system for Industrial IoT that uses context information alongside network information. Their system is shown to offer an increase in performance over non-context aware IDS, with a lower false positive rate overall. The authors successfully demonstrate the value of context awareness for IoT IDS, and suggest that context awareness should be considered more widely to increase the reliability of IoT intrusion detection systems.

Sharma et al [27] created a context aware system used for IoT-embedded Cyber Physical systems IDS, evaluated on an Unmanned Arial Vehicle. The system effectively uses context awareness to outperform similar systems in reliability and rates of false-positives, false-negatives, and true positives.

Sikder et al [28] developed a context aware sensor based attack detector for smart devices. This attack detector demonstrates the use of machine learning techniques for context aware IDS, and is evaluated on a smart phone. The authors use context in a way consistent with previously highlighted definitions, and can be viewed as an accurate example of context awareness use for IoT IDS.

Park et al [22] present a smart factory context aware IDS, however the authors introduce uncertainty as the work is identified as context aware, yet is also explicitly described as being based on situational awareness. This serves as an example of the confusion still present between context and situational awareness.

Pan et al [21] and Gopal and Parthasarathy [12] utilise context awareness for IDS within building management systems and wireless sensor networks respectively. Both examples utilise context awareness to achieve the goals of intrusion detection in a manner consistent with definitions. As both application areas contain large overlaps with IoT, these two examples should be considered when attempting to utilise context awareness for IoT.

Finally, Choi et al [8] implement context extraction to detect and identify faulty IoT devices. The author's use of context is not explicitly used for intrusion detection, however as the generated context information is used to provide services, the authors have successfully implemented context awareness according to definitions. While not designed for IDS, the approaches used within are easily adaptable for use in a different context.

While context awareness is a rich and varied area of research within IoT as a whole, literature surrounding its current use for IoT IDS is currently in its infancy. Understanding of context and its technical implementations within general literature is good, with the existence of artefacts such as the context life cycle serving to enable research within this space. Researchers are beginning to identify context awareness as a useful approach towards improving the

capability of current IDS for IoT, with implementations showing enhancement of reliability, false-positives, false-negatives, and true positives over non-context aware solutions. However, some confusion still remains surrounding its use, and in some cases its fundamental construct. Overall, the use of context awareness within IoT IDS shows promise, although there is much work still to be done.

4 Situation and Situational Awareness

4.1 Definitions

Compared to context and context awareness, definitions of situation and situational awareness do not have as great a presence or understanding within existing literature. There are, however, common themes that pervade provided definitions and support in their understanding.

In their work on situation aware access control, Kayes et al [13] propose that to specify a situation, it is required to capture the states of relevant context entities along with their relationships. Combining this with other information available within the environment, Kayes et al [13] defined a situation as consisting of the set of elementary information. This view is corroborated by Goker et al [11], who view context as a description of the aspects of a situation. While not necessarily a direct definition of situation, it can be taken from Kayes et al [13] and Goker et al [11] that a situation must, at the very least, contain context to be identified as such. This can then be substantiated further by Ye et al [30], who state that a situation can be seen as an abstraction of the events occurring in the real world derived from context. Transforming this into a formal construct, Meissen et al [19] define situation as $S = (t_{beg}, t_{end}, cs)$ where S is the situation, t_{beg} is the starting time of the situation, t_{end} is the end time of the situation, and cs is a set of characteristic features, with a characteristic feature viewed as a logical proposition about a context, or a subset of its components. From these examples we can conclude that for a situation to exist, it must implicitly contain context information. This information must be understood, processed, and combined to comprehend what the current situation at a specific point in time is. Rewording Meissen et al's [19] formal definition into Definition 3, a situation is therefore:

"a set of characteristic features over an identified time that can uniquely describe the real world scenario that is of current interest"

Situational awareness is less prevalent than context awareness in existing literature, potentially due to its use as a synonym within context definitions. Endsley [9] can be considered an early adopter of situational awareness, provided a widely accepted definition, Definition 4, as:

"the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"

While Endsley's [9] original definition was created for military purposes, its applicability to the field of computing, and more specifically IoT, is valid. Achieving

Endsley's [9] view of situational awareness would allow for improved user interaction, and the prediction of required services and resources before they are requested. Other definitions of situational awareness do exist within IoT focused literature [2], however, similarly to context and context awareness, our selected definitions are more generically applicable and thus better suited for IoT IDS.

4.2 Situation and Situational Awareness For IoT IDS

Of particular importance to situational awareness for IoT IDS is the conceptual model of Network Security Situation Awareness (NSSA) developed by Xu et al [29], formed through a combination of Endsley's [9] situational awareness model and Bass' [4] JDL model. Consisting of three levels, security situation perception, situation evaluation, and situation prediction, the model was developed specifically with IoT in mind. Expanding on this, Xu et al [29] focus on the first two levels and develop a situation reasoning framework, before demonstrating how it could detect attacks, worms, and evaluate IoT network vulnerabilities. The framework consists of 3 main components: a NSSA ontology, a reasoning engine, and user defined rules. Heterogeneous information, including context information, is formatted and fed into the ontology model, which models inputted information and the relationships existing between data points. Once the ontology is populated, the reasoning engine reasons out abnormalities using instances and user defined rules that identify different scenarios (e.g. attack scenarios). These three components combine to partially achieve the first two levels of NSSA, however Xu et al's approach [29] cannot monitor the overall security of IoT, as it does not contain the capabilities to handle all relevant information.

Utilising Xu et al's [29] conceptual model, Liu and Mu [17] present a network security situation awareness model using risk assessment methodologies. While the authors provide a starting point for this research area, the developed model simply scans a target network to obtain vulnerability information, assesses the risk value using their own custom formulas, then computes the network risk level based on the risks of all connected assets. As such, this model is limited and does not achieve true situational awareness.

McDermott et al [18] correctly identify and utilise situational awareness, however from the perspective of a device owner's awareness of a cyber attack on their device. The authors make no mention of NSSA, and instead utilise Endsley's [9] original model. Casillo et al [7] use situational awareness terminology, however the authors fail to demonstrate any implementation of situational awareness. Gendreau [10] demonstrates in depth understanding of situational awareness and its potential application to IoT IDS, however the author only suggests that their work is applicable to it from their given application of a self-reliant management and monitoring wireless sensor network cluster head selection algorithm.

Kirupakar and Shalinie [14] present a situation aware IDS design for industrial IoT gateways. The authors appear to have confused situation awareness with context awareness, as there is little to no mention of situational awareness within their work, instead they utilise a context analyser in their system and appear to be attempting to achieve context awareness.

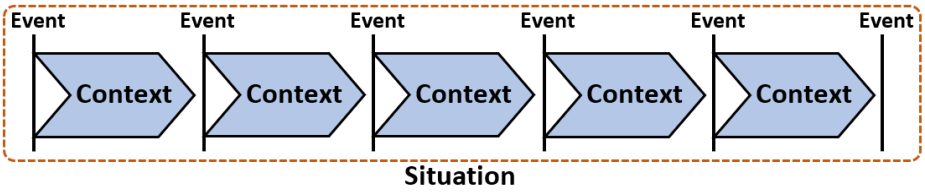

Figure 1. Depiction of relation between events, context, and situation

Similar to context and context awareness, literature for situational awareness within IoT IDS is currently in its infancy. There are examples of models designed to achieve situational awareness for IoT IDS, such as NSSA, although there is no general adoption of one specific model. Furthermore, there are concrete examples of situational awareness for IoT IDS, albeit a small number. While this means that researchers are beginning to identify its use for improving IoT intrusion detection, there is still confusion surrounding the exact nature of situational awareness and the difference between it and context awareness, with works in this area confusing the two. Overall, the use of situational awareness within IoT intrusion detection shows promise, encompassing and expanding the previously shown benefits of context awareness due to it including context awareness in its creation. However,it is in a much earlier stage than that of context awareness from both a theoretical and technical perspective, and as such the potential benefits of situational awareness for IoT IDS remain largely unexplored.

5 Comparison

Context and situational awareness concepts can be difficult to separate, as shown by the aforementioned definitions, where context requires the acknowledgement of a situation. Within existing literature, there are works that understand and utilise context awareness, yet do not consider situational awareness. Moreover, as previously demonstrated, there is a degree of confusion within context and situational awareness literature surrounding the difference between the two distinct concepts, with authors claiming to implement one, while actually implementing the other. There exists further evidence of separation between context and situational awareness in the National Institute of Standards and Technology's (NIST) framework and roadmap for smart grid interoperability standards [20]. In this document, NIST identify situational awareness as one of the top eight priority areas to be considered when protecting critical infrastructure, with a focus on smart grids. This example, and the previously described body of literature, form a basis towards the conclusion that context and situational awareness are two separate, yet interlinked entities, and not merely interchangeable concepts. This conclusion forms the basis for the following figures.

Figure 1 depicts the relationship between events, context, and a situation. As shown in Definition 3, a situation is a set of characteristic features over an identified time, that uniquely describes the real world scenario that is of current interest. Combined with Definition 1, which describes context as any information that can be used to characterise the situation of an entity, it is logical to reason that a situation's characteristic features must contain context.

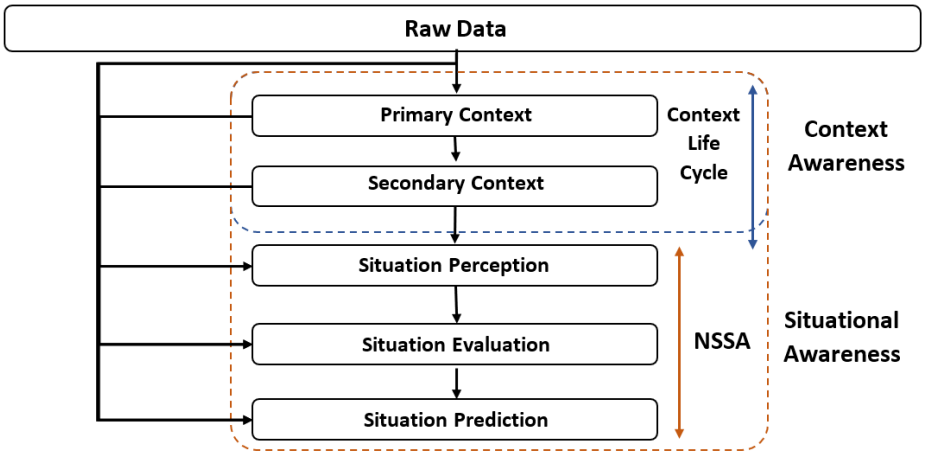

Figure 2. Pathway from raw data through to situational awareness

From Definition 4, it can be seen that context is a data source understood at a specific snapshot of time, while a situation develops and evolves over a period of time, thereby meaning that a situation is composed of context available within a specific window of time. Within a situation there can be many different contexts available and of use in understanding the situation, while context itself is implicitly tied to characterising the specific situation in question.

Expanding this relationship through to context and situational awareness, Definition 2 states that a system is context aware if it uses context to provide relevant information and/or services. According to Definition 4, situational awareness involves perceiving the situation, which as previously mentioned contains context within its set of characteristic features. Therefore, if a system implements situational awareness then it must intrinsically implement context awareness by default, as context is part of a situation and thereby used to provide relevant information. Figure 2 demonstrates this relationship and provides a theoretical pathway from raw data through to an understanding of a situation, based on the aforementioned conclusions and previously described differentiation between raw data, primary context, and secondary context. As context information is a building block in the understanding of a situation, the progression from both primary and secondary context towards understanding the current situation is natural. This viewpoint is partially substantiated by Perera et al [23], who when discussing primary and secondary context note that secondary context without primary context could indicate a less than complete understanding of the situation. Finally, the figure also highlights where current aspects of literature, such as the context life cycle and NSSA reside.

With a situationally aware system inherently implementing context awareness, it stands to reason that previously highlighted benefits of context aware IDS for IoT such as improved reliability, false-positives, false-negatives, and true-positives would be present within such a system. Furthermore, as a situation requires the understanding of a much larger set of information than purely con-

text, we believe that situationally aware IoT IDS would provide a more complete and holistic approach to IDS for IoT.

6 Conclusion

In this paper we have discussed the differences between context and situational awareness, identified by the current state of the art for both areas. This formed a basis to provide a discussion on how situational awareness implicitly utilises context awareness. Moreover, as situational awareness provides a more holistic and complete view of the security situation for an IoT environment, we suggest that future work implementing these concepts within IDS for IoT focus primarily on situational awareness and the use of context as a core constituent. We have identified that literature for context awareness in IoT is more developed than that of situational awareness, however common to both is a lack of literature surrounding their application towards IoT IDS, with both areas in their infancy. Although this area is in its early stages of development, authors are beginning to identify the benefits situational and context awareness can bring to IoT IDS. Finally, we have provided a pathway supporting the transformation of raw data towards situational awareness, including the use of context information as a core component. Our future work will focus on the practical implementation of this pathway to develop an IDS that is situationally aware, offering an enhanced viewpoint to further improve decision making processes and attack detection.

References

[1] Abowd, G.D., Dey, A.K., Brown, P.J., Davies, N., Smith, M., Steggles, P.: Towards a better understanding of context and context-awareness. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) **1707**(3), 304–307 (1999). https://doi.org/10.1007/3-540-48157-5_29

[2] Alcaraz, C., Lopez, J.: Wide-area situational awareness for critical infrastructure protection. Computer **46**(4), 30–37 (2013). https://doi.org/10.1109/MC.2013.72

[3] Anton, S.D., Fraunholz, D., Schotten, H.D., Teuber, S.: A question of context: Enhancing intrusion detection by providing context information. Joint 13th CTTE and 10th CMI Conference on Internet of Things - Business Models, Users, and Networks **2018-Janua**, 1–8 (2017). https://doi.org/10.1109/CTTE.2017.8260938

[4] Bass, T.: Intrusion detection systems and multisensor data fusion. Communications of the ACM **43**(4), 99–105 (2000). https://doi.org/10.1145/332051.332079

[5] Benkhelifa, E., Welsh, T., Hamouda, W.: A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems. IEEE Communications Surveys and Tutorials **20**(4), 3496–3509 (2018). https://doi.org/10.1109/COMST.2018.2844742

[6] Bricon-Souf, N., Newman, C.R.: Context awareness in health care: A review (2007). https://doi.org/10.1016/j.ijmedinf.2006.01.003

[7] Casillo, M., Coppola, S., De Santo, M., Pascale, F., Santonicola, E.: Embedded Intrusion Detection System for Detecting Attacks over CAN-BUS. 2019 4th International Conference on System Reliability and Safety, ICSRS 2019 pp. 136–141 (2019). https://doi.org/10.1109/ICSRS48664.2019.8987605

[8] Choi, J., Jeoung, H., Kim, J., Ko, Y., Jung, W., Kim, H., Kim, J.: Detecting and identifying faulty IoT devices in smart home with context extraction. Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018 pp. 610–621 (2018). https://doi.org/10.1109/DSN.2018.00068

[9] Endsley, M.R.: Toward a theory of situation awareness in dynamic systems (1995). https://doi.org/10.1518/001872095779049543

[10] Gendreau, A.A.: Situation awareness measurement enhanced for efficient monitoring in the Internet of Things. Proceedings - 2015 IEEE Region 10 Symposium, TENSYMP 2015 pp. 82–85 (2015). https://doi.org/10.1109/TENSYMP.2015.13

[11] Göker, A., Myrhaug, H., Bierig, R.: Context and Information Retrieval, chap. 7, pp. 131–157. John Wiley & Sons, Ltd (2009). https://doi.org/10.1002/9780470033647.ch7

[12] Gopal, R., Parthasarathy, V.: CAND-IDS: A Novel Context Aware Intrusion Detection System in Cooperative Wireless Sensor Networks by Nodal Node Deployment. Circuits and Systems **07**(11), 3504–3521 (2016). https://doi.org/10.4236/cs.2016.711298

[13] Kayes, A.S., Han, J., Colman, A.: PO-SAAC: A purpose-oriented situation-aware access control framework for software services. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) **8484 LNCS**, 58–74 (2014). https://doi.org/10.1007/978-3-319-07881-6_5

[14] Kirupakar, J., Shalinie, S.M.: Situation aware intrusion detection system design for industrial IoT gateways. ICCIDS 2019 - 2nd International Conference on Computational Intelligence in Data Science, Proceedings (2019). https://doi.org/10.1109/ICCIDS.2019.8862038

[15] Kouicem, D.E., Bouabdallah, A., Lakhlef, H.: Internet of things security: A top-down survey. Computer Networks **141**, 199–221 (2018). https://doi.org/10.1016/j.comnet.2018.03.012

[16] Liu, Y., Seet, B.C., Al-Anbuky, A.: An ontology-based context model for wireless sensor network (WSN) management in the internet of things. Journal of Sensor and Actuator Networks **2**(4), 653–674 (2013). https://doi.org/10.3390/jsan2040653

[17] Liu, Y., Mu, D.: A network security situation awareness model based on risk assessment, vol. 891. Springer International Publishing (2019). https://doi.org/10.1007/978-3-030-03766-6_3

[18] McDermott, C.D., Jeannelle, B., Isaacs, J.P.: Towards a conversational agent for threat detection in the internet of things. 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2019 (2019). https://doi.org/10.1109/CyberSA.2019.8899580

[19] Meissen, U., Pfennigschmidt, S., Voisard, A., Wahnfried, T.: Context- and situation-awareness in information logistics. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) **3268**, 335–344 (2004). https://doi.org/10.1007/978-3-540-30192-9_33

[20] National Institute of Standards and Technology: NIST Framework and Roadmap for Smart Grid Interoperability Standards , Release 3.0. Tech. rep. (2014). https://doi.org/10.6028/NIST.SP.1108r3

[21] Pan, Z., Hariri, S., Pacheco, J.: Context aware intrusion detection for building automation systems. Computers and Security **85**, 181–201 (2019). https://doi.org/10.1016/j.cose.2019.04.011

[22] Park, S.T., Li, G., Hong, J.C.: A study on smart factory-based ambient intelligence context-aware intrusion detection system using machine learning. Journal of Ambient Intelligence and Humanized Computing **11**(4), 1405–1412 (2020). https://doi.org/10.1007/s12652-018-0998-6

[23] Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Context aware computing for the internet of things: A survey. IEEE Communications Surveys and Tutorials **16**(1), 414–454 (2014). https://doi.org/10.1109/SURV.2013.042313.00197

[24] Sanchez, L., Lanza, J., Olsen, R., Bauer, M., Girod-Genet, M.: A generic context management framework for personal networking environments. 2006 3rd Annual International Conference on Mobile and

Ubiquitous Systems: Networking and Services, MobiQuitous (2006). https://doi.org/10.1109/MOBIQ.2006.340411

[25] Santos, L., Rabadao, C., Goncalves, R.: Intrusion detection systems in Internet of Things: A literature review. Iberian Conference on Information Systems and Technologies, CISTI **2018-June**, 1–7 (2018). https://doi.org/10.23919/CISTI.2018.8399291

[26] Sezer, O.B., Dogdu, E., Ozbayoglu, A.M.: Context-Aware Computing, Learning, and Big Data in Internet of Things: A Survey. IEEE Internet of Things Journal **5**(1), 1–27 (2018). https://doi.org/10.1109/JIOT.2017.2773600

[27] Sharma, V., You, I., Yim, K., Chen, I.R., Cho, J.H.: Briot: Behavior rule specification-based misbehavior detection for IoT-embedded cyber-physical systems. IEEE Access **7**, 1–25 (2019). https://doi.org/10.1109/ACCESS.2019.2917135

[28] Sikder, A.K., Aksu, H., Uluagac, A.S.: A context-aware framework for detecting sensor-based threats on smart devices. IEEE Transactions on Mobile Computing **19**(2), 245–261 (2020). https://doi.org/10.1109/TMC.2019.2893253

[29] Xu, G., Cao, Y., Ren, Y., Li, X., Feng, Z.: Network Security Situation Awareness Based on Semantic Ontology and User-Defined Rules for Internet of Things. IEEE Access **5**, 21046–21056 (2017). https://doi.org/10.1109/ACCESS.2017.2734681

[30] Ye, J., Dobson, S., McKeever, S.: Situation identification techniques in pervasive computing: A review. Pervasive and Mobile Computing **8**(1), 36–66 (2012). https://doi.org/10.1016/j.pmcj.2011.01.004

[31] Zarpelão, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C.: A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications **84**(September 2016), 25–37 (2017). https://doi.org/10.1016/j.jnca.2017.02.009