An Anomaly Detection Model for Ultra Low Powered Wireless Sensor Networks Utilizing Attributes of IEEE 802.15.4e/TSCH

Sajeeva Salgadoe and Fletcher Lu
Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, L1G-0C5, Canada
Email: sajeeva.salgadoe@uoit.ca; fletcher.lu@uoit.ca

Abstract—The rapid growth in sensors, low-power integrated circuits, and wireless communication standards has enabled a new generation of applications based on ultra-low powered wireless sensor networks. These are employed in many environments including health-care, industrial automation, environmental monitoring and intelligent transportation. Furthermore, a significant portion of low powered data requires a certain type of security that offers higher availability, confidentiality and data integrity. The objective of this work is to investigate the feasibility of using attributes of IEEE 802.15.4e/TSCH and machine learning techniques to determine traffic anomalies in ultra-low powered wireless networks. Several factors including the sample size, noise influence, classification algorithm and model aging process are investigated against prediction accuracy and other performance indicators. The experiments have demonstrated that machine learning models trained using carefully selected input features and adequate training data are able to detect traffic anomalies of low powered wireless networks with remarkable accuracy (over 95 percent), while keeping the false positive and negative rates to minimum.

Index Terms—LoWSN, LoWPAN, low powered sensor networks, IEEE 802.15.4e/TSCH, IoTs, wireless security, anomaly detection

I. Introduction

In recent years, a tremendous growth of solutions based on low powered wireless sensor devices has been witnessed [1]-[4]. Several factors including technological advancements, cost, simplicity and easy deployment have led to the unfolding of new dimensions, creating richer living experiences and economic benefits [5], [6]. Emerging paradigms such as Internet of Things (IoTs) and cloud computing have also significantly, contributed to the growth. The statistics indicate that as of 2016, there were over 6.4 billion such devices on the Internet, up 30 percent from previous year [5], [6].

In 2003, IEEE 802.15.4 standard was drafted by the Institute of Electrical and Electronic Engineers (IEEE) to define the Media Access Control (MAC) and Physical (PHY) layer specification for Low-Rate Wireless Personal Area Networks (LRWPAN) [7]; it has been widely used in low powered wireless network implementations. However, existing standards such IEEE 802.15.4 were unable to satisfy the emerging demand for super-low powered wireless requirements. IEEE 802.15.4 has defined a protection mechanism with the use of an Auxiliary Security Header (ASH) [7]. However, implementation of ASH in a low powered environment would drastically degrade the overall performance. According to previous research by Daidone *et al.* [1], use of ASH reduces 33.8 percent of the amount of data transmitted in a frame and increases energy consumption by 61.12 percent in 802.15.4 networks. Consequently, in 2012, IEEE defined a MAC amendment for 802.15.4 that was drafted as 802.15.4e to enhance functionality of 802.15.4-2006 and to better support industrial markets [8]-[10].

Despite the fact that threats associated with wireless sensor networks are complex [6], it is important to investigate different venues to secure sensor data. In this study, the feasibility of using the attributes of IEEE 802.15.4e, with the use of machine learning techniques to detect anomalies in wireless sensor networks is investigated.

II. Background

Ultra-Low powered Wireless Sensor Network (ULoWSN) is an evolving concept to satisfy emerging needs for low powered, embedded industrial applications [11]. ULoWSN consist of number of battery operated wireless sensor devices to measure environmental, physical or physiological properties in discrete time intervals for prolong periods (multiple years) without need for replacement of the batteries. Several researchers have investigated the energy consumption of low powered devices and according to their findings, regardless of effectiveness of radio transceivers, data transmission consumes significantly higher amount of energy compare to other activities [1].

A number of limitations in adapting conventional network protocols in ultra-low powered environments

Manuscript received October 27, 2018; revised March 28, 2019.
Corresponding author email: sajeeva.salgadoe@uoit.ca.
doi:10.12720/jcm.14.5.335-341

forced Institute of Electrical and Electronics Engineers (IEEE) to design a standard to operate effectively in low powered environments. Consequently, IEEE 802.15.4e has been drafted to enhance the Media Access Control (MAC) layer functionality to accommodate ultra-low-powered communication and it is considered as the latest generation reliable media access mechanism for low powered wireless networks [11]. The channel agility of wireless networks operating on IEEE 802.15.4e/TSCH mode provides higher reliability in noisy environments.

Several MAC behaviour methods are defined by 802.15.4e, namely DSME (Deterministic & Synchronous Multi-Channel Extension), LLDN (Low Latency Deterministic Network), TSCH (Time Slotted Channel Hopping), and AMCA (Asynchronous Multi-channel Adaptation) and they are tailored to satisfy various network requirements [11]. The TSCH maintains high reliability and low duty cycles, using time-synchronization and channel hopping. The TSCH mode has emerged from Time Synchronized Mesh Protocol (TSMP) [12] and High-way Addressable Remote Transducer (HART) [13] Technology. In Time Slotted Channel Hopping (TSCH) mode, nodes are synchronized to a slotframe structure and to a network coordinator, also known as the personal area network coordinator (PAN coordinator) [11]. The TSCH mode is primarily used in mesh environments, where some remote low powered nodes are unable to reach the central controller, directly. Furthermore, TSCH mode is specially tailored for environments with low throughput, high latency and small packet size requirement [11].

A slotframe is a group of time slots repeated over time and a time-slot is a predetermined period of time used by nodes to exchange data [11]. Each synchronized node follows a schedule, dictating the allowed operation for a particular node, during a timeslot. Each timeslot schedule specifies which two nodes are participating in data exchanged, using a specific channel [11]. Based on the schedule created by the PAN coordinator, an individual node can be put into transmit or receive mode, using a specific channel or switch to sleep mode [11]. TSCH is a deterministic protocol where nodes are only awake during timeslots which have assigned operations for a particular node. The following diagram is a slotframe with ten timeslots.

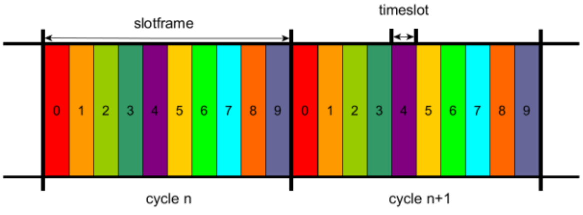


Fig. 1. IEEE 802.15.4e/TSCH slotframe

Each timeslot can be divided into multiple cells and the amount of cells is dependent on the available channel list. The channel list is formulated using a regulatory requirement and localized factors such as interference. Fig. 2 depicts a portion of a schedule which has a slotframe with ten timeslots and five usable channels. Each cell in a timeslot is assigned a node-pair to utilize a unique channel. However, each cell can be shared by multiple node-pairs using a contention access mechanism. A specific frequency for a particular cell is derived using following formula.

$freq_{active} = Freq_{list}$ [$(ASN + ch_{Ofset})$ mod $nrOf_{Channels}$] where

$freq_{active}$ = Active Frequency

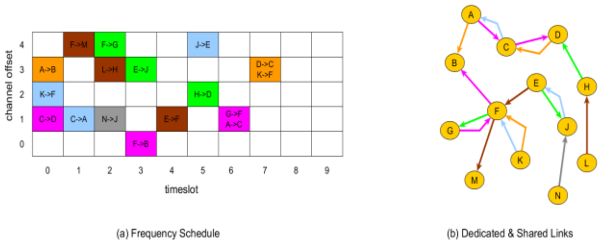
$Freq_{list}$ = Available usable frequencies

ASN = Absolute Slot Number (an unique number used by the TSCH to identify a timeslot and it indicates the total number of slots elapsed since the network was formed)

Ch_{offset} = Assigned by the PAN coordinator to a particular "link"

$nrOf_{channels}$ = Number of usable channels in channel list

The following diagram describes a sample TSCH schedule and corresponding activities in a wireless network operating in IEEE 802.15.4e TSCH mode. Each color represents a different frequency used for the communication.



channel offset										
4		F->M	F->G			J->E				
3	A->B		L->H	E->J				D->C K->F		
2	K->F					H->D				
1	C->D	C->A	N->J		E->F		G->F A->C			
0				F->B						
	0	1	2	3	4	5	6	7	8	9

(a) Frequency Schedule

(b) Dedicated & Shared Links

Fig. 2. IEEE 802.15.4e/TSCH schedule

Security Threats

There are several known attacks related to security protocols associated with open wireless standards. Attacks on 802.15.4/802.11 networks can be classified into several groups, based on the nature of the attacks, namely key retrieving attacks, availability attacks, keystream retrieving attacks and man in the middle (MiTM) attacks [14].

Availability related attacks are also known as Denial of Service (DOS) attacks and they are common to most versions of the IEEE 802.11 and 802.15.4 protocol family [14]. Attackers attempt to exhaust network resources or resources of a specific host to create a denial of service. Since management frames are sent unprotected, most DOS attacks on open standard networks are based on broadcast of forged management frames [14]. However, lack of adequate physical security controls could also lead to DOS attacks. For instance, vandalism, natural disasters and unintentional accidents could disrupt the availability of low powered sensor data. De-authentication attack is one of the most common

DOS attacks on open standard networks [14]. The attacker monitors the wireless traffic for MAC addresses of client stations, which can be found in unprotected management frames and send forged de-authentication messages to clients on behalf of the AP. However, it is also possible to send a forged de-authentication message on behalf of clients to an AP. Disassociation attacks [14] are similar to de-authentication attacks and they utilize disassociation messages instead of de-authentication messages. De-authentication broadcast attacks [14] are also similar to de-authentication attacks. However, this particular attack type uses broadcast MAC addresses as the destination address and as a consequence all clients in the network are forced to re-authenticate. The block acknowledgement flood attack takes advantage of Add Block Acknowledgment (ADDBA) and was introduced in the 802.1n protocol [14]. ADDBA allows a client to send a larger block of data without fragmentation. However, an attacker could send an ADDBA request on behalf of a client, which negotiates the block size and the sequence numbers, associated with those blocks [14]. The authentication request flooding attack is based on flooding the client association table with fake authentication requests and eventually, the AP will not be able to respond to legitimate authentication requests, in a timely manner [14]. Beacon flood attacks are based on advertising the sequence of fake ESSIDs (Extended Service Set Identification) to overflow the list of available networks [14]. The attacker could send a sequence of fake probe requests to overwhelm the AP and cause an attack known as a probe request flooding attack [15]. A probe response flooding attack is also a common DOS attack on open standard networks [15]. The attacker replies to probe request messages by acting as a valid AP.

Man in the middle attacks (MiTM) are based on impersonation techniques. For instance, Honeypots are created by security administrators to attract attackers and redirect their attention from legitimate targets. However, intruders use the same technique to create malicious wireless networks in order to attract users. Using MiTM attacks, adversaries may be able to monitor an entire communication, including application level data, such as passwords and personal information. However, if the communication is secured using an upper layer control such as Secure Sockets Layer (SSL), an attacker still could launch a replay attack to create havoc. Evil Twin is also a different variance of honeypot approach by advertising an AP with same network name (SSID) to mislead legitimate clients [16].

III. Related Work

Most proposed solutions to prevent the aforementioned attacks are based on modifications of existing standards, which may lead to inconsistency with open standards. Some studies have been conducted to develop external systems, such as Intrusion Detection System (IDS) to detect attacks related to wireless networks. F. Ferreri *et al.* [15] have demonstrated how easy it is to launch a DOS attack on open standard networks, using Authentication Request Flood (ARF), Association Request Flood (ASRF) and Probe Request Flood (PRF). L. Wang *et al.* [16] discusses a DOS attack on 802.11i, using a 4-way handshake protocol [17] and a possible solution, based on 3-way handshake mechanism, using authenticated management frames. B. Aslam et al. [18] also proposes a solution to disassociation DOS attacks using authenticated management messages. However, both those solutions require modifications to the firmware of the wireless interface card. Z. Afzal *et al.* [19] suggests a method to mitigate de-authentication attacks and Evil Twin Attacks using a signature based Intrusion Detection System. Detection of de-authentication based DOS attacks and a prevention mechanism using intrusion prevention mechanism is discussed by M. Agarwal et al. [20]. Previous work by M. Agarwal *et al.* [20] has been improved by M. Agarwal et al. in literature [21] by implementing a machine learning technique to detect DOS based on de-authentication attacks. Research work by C. Panos *et al.* [22] discusses a specification-based intrusion detection mechanism which uses both signatures and anomalies to detect attacks on Ad-Hoc networks. However, most proposed solutions to mitigate attacks on wireless networks are based on protocol modification, firmware upgrades or via a middleware solution.

M. L. Das *et al.* [23] proposes a two factor, user authentication mechanism using a one-way hash function and XOR operation. Authors of the work insist that the proposed method can prevent password guessing, impersonation and replay attacks. M. K. Khan *et al.* [24] suggested an enhancement to [27] [23] by addressing some of the flaws related to password modification and vulnerabilities related to privileged, insider attacks. However, both above solutions require modification to the low powered node software. L. H. Freitas *et al.* [25] proposes a hybrid encryption mechanism, based on both symmetric and asymmetric keys, with the use of a message authentication mechanism, to secure the sensor data. R. Daidone *et al.* [26] suggests a modular middleware solution to guarantee the confidentiality, integrity and the authenticity of low powered sensor data. G. Piro *et al.* [27] discusses a lightweight mechanism to negotiate link keys in 802.15.4 networks; however, low powered device software has to be modified to accomplish the key, negotiation process. F. X. Standaert *et al.* [28] discusses the use of an efficient low powered security implementation in an application-specific integrated circuit (ASIC), which can be used in low powered devices. However, these types of solutions require a complete re-design of the device’s hardware architecture. T. Hao *et al.* [29] proposed a forecast model of a security situation in low powered wireless networks. Their approach is based on a probabilistic model (Hidden Markov model) to forecast the security posture of a given situation. A. F. Skarmeta *et al.* [5] discusses a decentralized mechanism, to protect data privacy, in low powered wireless networks. Their solution is based on the use of a lightweight token, to access network resources and an optimized implementation of the elliptic curve algorithm is required in each node. L. Marin *et al.* [30] also, proposed a solution based on ECC (Elliptic Curve) for the Internet of Things (IoTs).

IV. Research Design & Methods

Due to resource restrictions and limited operational capabilities, ultra-low powered wireless sensor networks tend to create more deterministic behaviour patterns compared to conventional wireless networks. These behaviour patterns can be used to identify a finite number of contexts for a low powered wireless network. Subsequently, context data can be used to determine acceptable baseline values for normal operation and to detect outliers and anomalies of corresponding low powered wireless network. Different approaches including rule based and machine learning can be used to identify the set of behavioural contexts of a particular ULoWSN. However, in this work, several machine learning techniques are evaluated to construct most effective model to detect traffic anomalies in ULoWSNs.

Data Collection

OpenWSN is used to generate data associated with low powered nodes operating in TSCH mode. Network topology is manually created and the link quality and packet drop rate (PDR) are manually adjusted to simulate a realistic network environment. An unofficial draft of 6TiSCH, implemented by OpenWSN is used to provide IPv6 support for IEEE 802.15.4e/TSCH network. Furthermore, OpenWSN also provides an simplified implementation of a TSCH scheduling mechanism. In an OpenWSN simulation environment, the PAN coordinator and the root node for the RPL based routing process is manually selected. RPL generates a routing structure based on a rank based mechanism. Once a suitable root node is selected, RPL initiates the route formation process by generating a Destination-Oriented Directed Acyclic Graph (DODAG) for each node. A third party dissector has been used by the Wireshark to identify wireless packets operating in TSCH mode.

Absolute Slot Number (ASN) is used by wireless networks operating in IEEE 802.15.4e TSCH mode to uniquely identify a timeslot used by a particular packet. Furthermore, a single time-slot is partitioned into multiple cells to facilitate multiple communications during a single timeslot using different channels. The ASN is transmitted in the payload section of the Information Element in Enhanced Beacon packets [13] [11]. Even though, each active node is able to determine the active ASN by analysing the last received Enhanced Beacon, according to IEEE 802.15.4e/TSCH, nodes are not obliged to retransmit the ASN in a unicast data exchange.

In this work, the four machine learning algorithms (Support Vector Machines (SVM), K-Nearest Neighbours (KNN), Neural Networks (NN) and Decision Tree (DT)) are used to build classification models. Several factors, including training set size, classification algorithm and model aging process are tested to determine the impact on prediction accuracy.

V. Result

Sample Size

The following experiment is performed using four default classifiers (SVM, KNN, NN and DT) and several training sets. The experiments are based on a sequence permutation technique to generate anomalous data. The following diagram compares the prediction accuracy of different training sets for each classification algorithm.

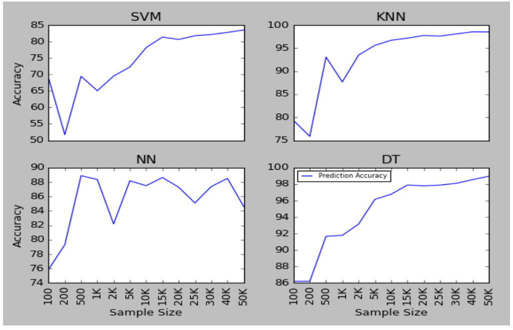


Fig. 3. Training set size vs prediction accuracy

Fig. 3 demonstrates a positive correlation between prediction accuracy and the training set size with prediction models based on all except neural network classification models. However, neural networks based models are able to maintain consistent accuracy with prediction models, trained with 500 or more samples

Noise Threshold

Different causes may contribute to spikes in data flow, including hardware failure, interference, network congestion, intentional/unintentional sabotage and battery drainage. Recurrent impacts such as seasonal effects can be learned by classification models trained with larger data sets. While larger data sets produce a higher variance, smaller data sets are inclined to bias predictions. In the following experiments, a controlled random noise is introduced to the test data as a stress-test on the prediction model. Random noise is retrieved from a normally distributed noisy-sample-set, parameterized (controlled) by the standard deviation. The following experiment is performed using the four default classification algorithms, with a 5000-sample unchanged training set.

The following diagram demonstrates the corresponding result.

The above diagram demonstrates a significant drop in prediction accuracy with a higher variance of test data noise. It confirms that prediction models, based on all four algorithms, are unable to identify unseen data with a higher noise variance, accurately. (Fig. 4)

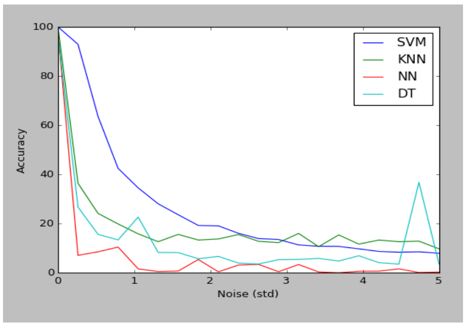


Fig. 4. Data variance vs prediction accuracy

The following diagram is generated, using prediction models based on a Decision Tree model. The purpose of the following experiment is to examine the correlation between the variance of unseen data and the prediction accuracy of models trained with different sized training sets (range 100 - 50000 samples). The variance is measured using standard deviation value used in Gaussian distribution function to generate anomalous data samples.

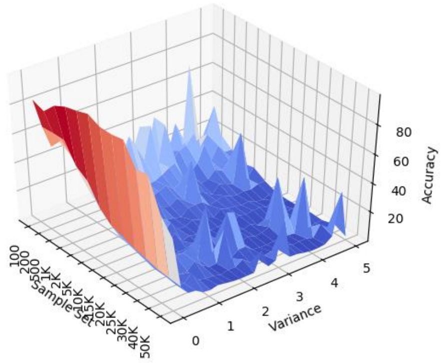


Fig. 5. Data variance (STD) vs training set size vs prediction accuracy

The above diagram confirms that regardless of the training set size, prediction accuracy drastically diminishes with a higher variance of unseen data. (Fig. 5)

The objective of the following experiment is to examine the correlation between input data variance (noise), training set size and the prediction accuracy for a Random Forest model. The data noise is controlled using the standard deviation value of Gaussian distribution function.

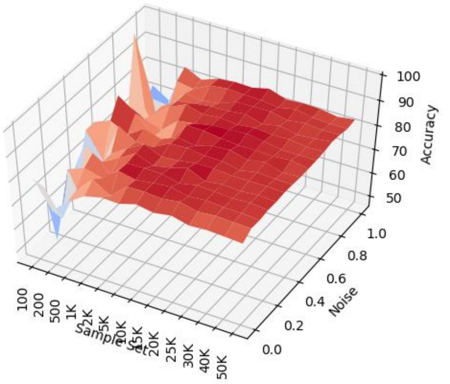


Fig. 6. Data variance vs training set size vs prediction accuracy

The above result demonstrates an inconsistent relationship between prediction accuracy and input data variability (noise) for models trained using smaller training sets. However, models with larger training sets are able to produce consistent accuracy, regardless, of the input data variance. (Fig. 6)

Model Aging Process

A reliable prediction model should be able to maintain high prediction accuracy and other metrics such as false positive and negative rates that are fairly consistent over extended periods of time. In the following experiment, the prediction model's aging process is investigated. In this experiment, a number of test-sets with 2000 samples in each, collected in predetermined time intervals over prolonged periods, are used. Four default classification algorithms are used to train prediction models with three different training sets (2000, 5000 and 10000 samples), collected from the same network, at time zero (t0). Corresponding results are depicted in Fig. 7.

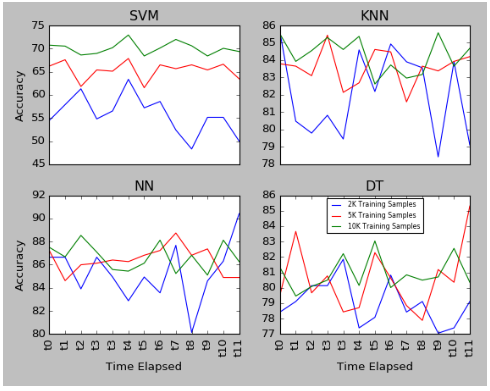


Fig. 7. Prediction model aging process

Fig. 7 illustrates that most models are able to maintain prediction accuracy with a marginal degradation during the test period. Furthermore, models trained with smaller datasets, demonstrate a higher variance of prediction accuracy and models trained with a larger data set, gravitates to more stable accuracy rates.

Resource Utilization

In the following, our four default classification algorithms are examined for resource consumption. Three performance indicators (CPU usage, time, memory usage) are tested and the following diagram describes the corresponding result.

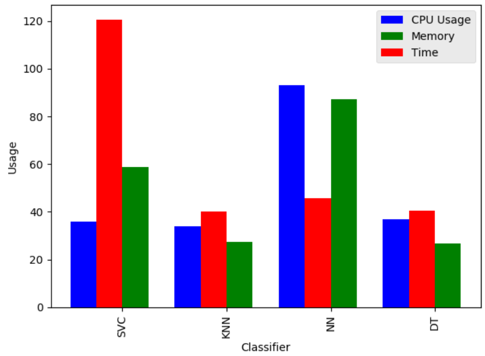


Fig. 8. Resource utilization by classifiers

The results of Fig. 8 confirm that the prediction models based on SVM require a significantly longer period for the training process. In the meantime, the NN based models utilizes higher computational power during the training process. However, models based on KNN and DT, are able to utilize less total resources while providing similar performance.

VI. Conclusion

In this work, IEEE 802.15.4e/TSCH attributes were evaluated to build a model to identify traffic anomalies in low powered wireless networks. Several characteristics including input parameters, training set size, input data variance and model aging processes were investigated. Experimental results indicate that significant prediction accuracy can be achieved by utilizing ASN and timestamps to build a traffic anomaly detection model using machine learning. This model could be further enhanced by associating various low powered wireless characteristics such as battery usage, packet payload values, source/destination identities as well as physical layer attributes including RSSI, Link Quality, Link Distance, and RF Noise values.

References

[1] R. Daidone, G. Dini, and M. Tiloca, "On experimentally evaluating the impact of security on IEEE 802.15.4 networks," in *Proc. International Conference on Distributed Computing in Sensor Systems and Workshops*, 2011, pp. 20-25.

[2] D. De Guglielmo, A. Seghetti, G. Anastasi, and M. Conti, "A performance analysis of the network formation process in IEEE 802.15.4e TSCH wireless sensor/actuator networks," in *Proc. Symposium on Computers and Communication*, 2014, pp. 23-26.

[3] M. Lemmon, Q. Ling, and Y. Sun, "Overload management in sensor actuator networks used for spatially-distributed control systems," in *Proc. 1st International Conference on Embedded Networked Sensor Systems*, ACM, 2003.

[4] J. Xu, G. Yang, Z. Chen, and Q. Wang, "A survey on the privacy-preserving data aggregation in wireless sensor networks," *China Communications*, vol. 12/5, pp. 162–180, 2015

[5] A. F. Skarmeta, J. L. Hernández-Ramos, and M. V. Moreno, "A decentralized approach for security and privacy challenges in the Internet of Things," in *Proc. IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 67–72.

[6] M. J. Covington and R. Carskadden, "Threat implications of the Internet of Things," in *Proc. 5th International Conference on Cyber Conflict*, 2013, pp. 1-12.

[7] IEEE std. 802.15.4, Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Standard for Information Technology, 2006.

[8] J. Zhou, A. E. Xhafa, R. Vedantham, R. Nuzzaci, A. Kandhalu, and X. Lu, Comparison of IEEE 802.15.4e MAC features 2014 IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 203–207.

[9] E. Vogli, G. Ribezzo, L. A. Grieco, and G. Boggia, "Fast join and synchronization schema in the IEEE 802.15.4e MAC," in *Proc. IEEE Wireless Communications and Networking Conference Workshop*, 2015, pp. 85-90.

[10] M. Henze, L. Hermerschmidt, D. Kerpen, R. Häußling, B. Rumpe, and K. Wehrle, "User-Driven privacy enforcement for cloud-based services in the internet of things," in *Proc. International Conference on Future Internet of Things and Cloud*, 2014, pp. 191-196.

[11] IEEE std. 802.15.4e, Part. 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC Sublayer, IEEE Standard for Information Technology, 2012

[12] K. Pister and L. Doherty, "TSMP: Time synchronized mesh protocol," in *Proc. International Symposium of Distributed Sensor Networks*, Florida, USA, Nov. 2008.

[13] HART Communication Protocol and Foundation. [Online]. Available: http://www.hartcomm2.org

[14] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset," *IEEE Communications Surveys & Tutorials*, vol. 18/1, pp. 184–208, 2016.

[15] F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks," in *Proc. IEEE Wireless Communications and Networking Conference*, vol. 1, 2004, pp. 634–638.

[16] L. Wang and B. Srinivasan, "Analysis and improvements over dos attacks against IEEE 802.11i standard," in *Proc. Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, vol. 2, 2010, pp. 109-113.

[17] C. He and J. C. Mitchell, "Analysis of the 802.11i 4-Way Handshake," in *Proc. 3rd ACM Workshop on Wireless Security*, Philadelphia, PA, USA, pp. 43 – 50, 2004

[18] B. Aslam, M. H. Islam, and S. A. Khan, "Pseudo randomized sequence number based solution to 802.11 disassociation denial of service attack," in *Proc. First Mobile Computing and Wireless Communication International Conference*, Amman, 2006, pp. 215-220.

[19] Z. Afzal, J. Rossebø, B. Talha, and M. Chowdhury, "A wireless intrusion detection system for 802.11 networks," in *Proc. International Conference on Wireless Communications, Signal Processing and Networking*, 2016, pp. 828-834.

[20] M. Agarwal, S. Biswas, and S. Nandi, "Detection of De-authentication denial of service attack in 802.11 networks," in *Proc. Annual IEEE India Conference*, 2013, pp. 1-6.

[21] M. Agarwal, S. Biswas, and S. Nandi, "Detection of De-authentication dos attacks in Wi-Fi networks: A machine learning approach," in *Proc. IEEE International*

Conference on Systems, Man, and Cybernetics, 2015, pp. 246–251.

[22] C. Panos, P. Kotzias, C. Xenakis, and I. Stavrakakis, "Securing the 802.11 MAC in MANETs: A specification-based intrusion detection engine," in *Proc. 9th Annual Conference on Wireless On-Demand Network Systems and Services*, 2012, pp. 16-22.

[23] M. L. Das, "Two-Factor user authentication in wireless sensor networks IEEE transactions," *Wireless Communication*, vol. 8, pp. 1086-1090, 2009.

[24] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'Two-Factor user authentication in wireless sensor networks," *Sensors*, vol. 10/3, pp. 2450-2459, 2010.

[25] L. H. Freitas, K. A. Bispo, N. S. Rosa, and P. R. F. Cunha, "SM-Sens: Security middleware for wireless sensor networks," in *Proc. Information Infrastructure Symposium*, 2009.

[26] R. Daidone, G. Dini, and M. Tiloca, "STaR: A reconfigurable and transparent middleware for WSNs security," in *Proc. 2nd International Conference on Sensor Networks*, 2013.

[27] G. Piro, G. Boggia, and L. A. Grieco, "A standard compliant security framework for IEEE 802.15.4 networks," in *Proc. IEEE World Forum on Internet of Things (WF-IoT)*, 2014, pp. 27-30.

[28] F. X. Standaert, G. Rouvroy, J. J. Quisquater, and J. D. Legat, "A methodology to implement block ciphers in reconfigurable hardware and its application to fast and compact AES RIJNDAEL," in *Proc. International Symposium on Field-Programmable Gate Arrays*, Monterey, CA, 2003.

[29] T. Hao, Y. Jia, and X. Tian, "Research on the forecast model of security situation for information system based on Internet of things," in *Proc. International Conference on Anti-Counterfeiting, Security and Identification*, 2013, pp. 1-5.

[30] L. Marin, A. Jara, and A. F. Skarmeta, "Shifting primes: Optimizing elliptic curve cryptography for smart things," in *Proc. Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2012, pp. 793–798.

Sajeeva Salgadoe is a PhD candidate at University of Ontario Institute of Technology in Canada. He received his master degree in Computer Science from Warsaw University of Technology Poland. His research interests include machine learning, security and low powered sensor networks.

Dr. Fletcher Lu is an associate professor with the University of Ontario Institute of Technology in Canada. He received a Bachelor of Math degree in Computer Science and Masters of Math degree in Scientific Computation and a PhD in Artificial Intelligence from the University of Waterloo. His research specializes in numerical computation and machine learning with applications in Health and Business.