Improving Cellular IoT Security with Identity Federation and Anomaly Detection

Bernardo Santos
OsloMet – Oslo Metropolitan University
Oslo, Norway
e-mail: bersan@oslomet.no

Bruno Dzogovic
OsloMet – Oslo Metropolitan University
Oslo, Norway
e-mail: bruno.dzogovic@oslomet.no

Boning Feng
OsloMet – Oslo Metropolitan University
Oslo, Norway
e-mail: boningf@oslomet.no

Niels Jacot
Wolffia AS
Helsinki, Finland
e-mail: n.jacot@wolffia.net

Van Thuan Do
Wolffia AS
Oslo, Norway
e-mail: vt.do@wolffia.no

Thanh Van Do
Telenor & OsloMet – Oslo Metropolitan University
Fornebu, Norway
e-mail: thanh-van.do@telenor.no

***Abstract*—As we notice the increasing adoption of Cellular IoT solutions (smart-home, e-health, among others), there are still some security aspects that can be improved as these devices can suffer various types of attacks that can have a high-impact over our daily lives. In order to avoid this, we present a multi-front security solution that consists on a federated cross-layered authentication mechanism, as well as a machine learning platform with anomaly detection techniques for data traffic analysis as a way to study devices' behavior so it can preemptively detect attacks and minimize their impact. In this paper, we also present a proof-of-concept to illustrate the proposed solution and showcase its feasibility, as well as the discussion of future iterations that will occur for this work.**

Keywords-machine learning; anomaly detection; mobile network security; IoT security; cross layer security

I. INTRODUCTION

Cellular IoT has become a more known concept as we're seeing more devices and solutions that rely on its related technologies, and this will continue to expand as we see more smart-home, e-health and other types of applications becoming more available to users worldwide.

Although these devices are connected through a Subscriber Identity Module (**SIM**) card, weak authentication methods are used to connect them to their corresponding platforms and still to this day these devices are targeted for various types of attacks and exploits, which can create a massive impact not only in the solution they belong to, but also, it can target different sectors as it is able to spread through the network, causing undesirable effects in our daily life.

To this end, an integrated security mechanism consisted by a cross-layered authentication method and an identity federation as well as a machine learning platform for anomaly detection on data traffic is presented with the aim of secure connected devices and to identify possible exploits and attacks to contain and mitigate them, as well as isolate infected devices from affecting others.

This paper starts by briefly discussing the concepts of Cellular IoT and Identity Federation in section II, giving a bit more relevance to the machine learning and anomaly detection component in III. In IV and V, we present our proposed solution and implemented proof-of concept and to finalize, in VI and VII we discuss the next steps for this work and make some final remarks.

II. SHORT ABOUT CELLULAR IOT AND IDENTITY FEDERATION

A. Cellular IoT

Cellular Internet of Things (**C-IoT**) is a concept that illustrates the process of supporting common **IoT** connections and services (e.g. smart-home, e-health,…) through existing mobile network infrastructures [1][2] resorting to technologies such as Narrowband IoT (**NB-IoT**), Cat. M, among others.

The behaviour of these devices isn't the same as your typical mobile device (e.g. smartphone) as they aren't necessary always connected to the network all the time, otherwise its performance would be affected due to excessive energy consumption. However, when they do connect in order to transmit their data to the corresponding platform, it should be devoided of disruptions and secure, so the data isn't prone to exploits and/or compromises.

B. Identity & Identity Federation

The concept of digital identity [3][4][5] comes as a way to centralize one's information into one generic identity that helps both individuals and corporations, since users don't

 DOI: http://dx.doi.org/10.1109/ICCCS49078.2020.9118438

need to create specific identities with a subset of parameters, since when signing up for a service for instance, only the relevant details are forwarded to such service, allowing to manage one's data in a more cohesive way.

This approach can also be extended to devices, as nowadays the same situation surfaces, in which devices are enrolled in various services and in some cases the parameters to create an identification for a device aren't clear. To that, an identity federation has to be considered as to align the identity that a device has from the mobile network [6] and unify it with the ones created in the Application layer. For that purpose, the following standards are considered:

1) OAuth 2.0

OAuth 2.0 [7] is a protocol that, by a user's consent, allows a third-party client to access resources (in a server, accessible through the network) on its behalf to facilitate the authentication process.

2) OpenID Connect

OpenID Connect [8] is considered an extension or a profile of OAuth 2.0 that offers single sign-on and identity provision on the internet. It enables client applications to verify the identity of the user based on the authentication performed by an OpenID Provider.

III. Machine Learning and Anomaly Detection for Cellular Networks

With the upcoming of the fifth generation of mobile networks (**5G**), it is predicted that the amount of devices connected in the network will raise exponentially and the data traffic generated from these devices will be immense. This *Big Data* that will surface from this new generation is something that mobile operators and cloud service providers are now addressing as how to manage such a massive amount of data without undermining the performance of both network and cloud infrastructures.

To this end, machine learning techniques are being considered due to the ability of, from the data that is fed to it, identify patterns, take actions and also learn and adapt given new scenarios. Machine learning in the context of **5G** networks come as a tool for a multitude of network related activities [9][10], from resource management, traffic classification, mobility pattern prediction and more related to our topic of interest, anomaly detection.

Machine learning anomaly detection is an approach that studies the data traffic by analysing behaviours and activities and from it detect and foreseen inconsistencies from what is assumed to be normal. As pointed out in [11], this will require powerful resources as to pick from all the data some type of "anomaly", which will need be validated at first by expertise staff. This means that a potential challenge is to try to define a device profile that can predict types of usage, data peeks and overall allowed but abnormal behaviours (e.g. users installing or uninstalling apps on their smartphones). Another challenge can also be the parameters to be considered as they are the basis from which profiles are created. If the parameters reveal to be insufficient or not good, that means a new profile must be conceived.

However, for most **IoT** devices, their behaviour doesn't suffer much changes (compared to other mobile devices) as they have a very specific pattern in the network of forwarding their payload to a specific and unique destination and then having their connection idle until another time-spaced programmable data transfer occurs.

In order to have a proper anomaly detection technique, it is necessary to consider the following:

A. Unsupervised Learning

The starting point from the data collected is to try to obtain some structure and patterns without providing any type of meaning to it [12], Unsupervised learning algorithms will analyze and form agglomerates of similar data as it starts to detect some similarity considering what was fed to it. From this, we're able to gather some more insightful information that we couldn't initially from the pre-processed data. The following algorithm is one of the most popular and used nowadays for many applications:

1) K-means algorithm

The K-means algorithm [13] is a partitional algorithm in which from a set of objects is minimized to a group of clusters that tries to include as much as data as possible. It is an iterational algorithm, so the number of clusters may vary whilst the algorithm is running. Each cluster will have a "centroid" which is the datum that the rest of the data in a cluster revolves around it, acting as the average or the mean of the cluster.

B. Anomaly Detection

After the clusters were established and it's feasible to start creating profiles for devices regarding their behaviour, it's possible to start having data going through anomaly detection algorithms. To simply put, an anomaly will be considered when a datum falls out from the clusters or simply does not have another correlation with the rest of the data. However, as mentioned earlier, at the beginning the process needs to be refined as the model may detect "anomalies" that when cross validated were only false positive. Tinkering with the model in terms of how lenient it such be (margin of error) and also the features/attributes to use will later determine the efficiency of the model. The following algorithms are the most popular nowadays:

1) k-NN Global Anomaly Detection

A straightforward algorithm to detect global anomalies, in which for every entry from the dataset, the k-nearest-neighbours are found and afterwards an anomaly score is given considering the existing neighbours. As stated in [14], the choice of the parameter k (number of clusters) will greatly determine the results as it is recommended to assign it between $10 < k < 50$. However, although the algorithm can achieve great results, it is not recommended to use when the dataset is too large, and the results are needed in a short amount of time (e.g. dealing with real-time network traffic data).

2) uCBLOF

Standing for unweighted cluster-based local outliner factor, this algorithm performs better when dealing with large datasets. Also described in [14], it uses clustering techniques

to determine dense data areas and performs an estimation factor for each cluster created. Afterwards, a heuristic is used to classify the size of the clusters and an anomaly score is given by the distance of each instance to the closest cluster center multiplied by the instances belonging to the cluster. Also, like in the aforementioned model, the value of k will influence the outcome.

3) S-H-ESD

An algorithm developed by *Twitter Inc* [15], the seasonal hybrid extreme studentized deviate model offers more adaptability for time series data that usually come from real-time generated traffic. The model assumes correctly a high rate of anomalies, regardless of the situation context an anomaly is found in. This is possible by considering statistics metrics such as the *median* and the median absolute deviation (MAD). This adaptability however comes at a small cost of performing a bit slower than other methods, but its results and accuracy overall makes this model the most used considering time series related data.

IV. PROPOSED SOLUTION

With the purpose of increasing security for IoT devices in a cross-layer fashion, we propose a implementation that has its main objective on mitigating exploits and attacks in multiple fronts. As established in [16], we have implemented an identity management system (**IDMS**) and developed an identity federation mechanism that allows to use known identifiers used in the cellular network and bring it towards the application layer, making it a multi-purpose identity. This implementation allows to have a grasp of a device's behaviour in a sense that some exploits an be addressed by having this link between both layers.

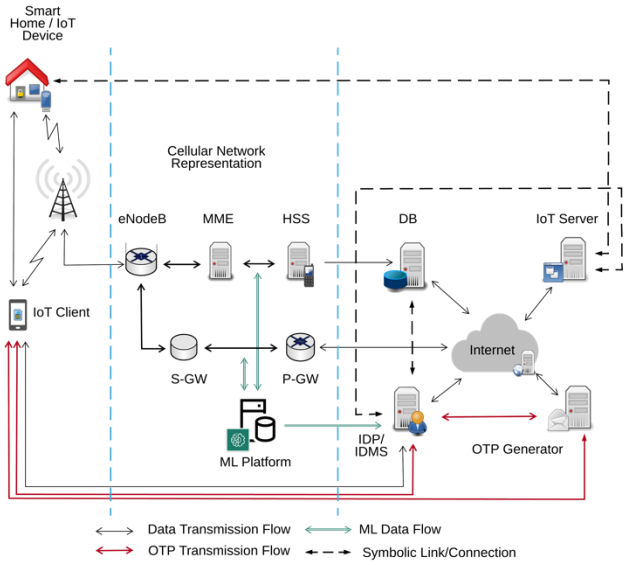

Figure 1. Illustration of the proposed solution.

However, with this work, our focus is to consider it as an extension as to be more pre-emptive, meaning to address attacks much earlier from the network layer in this phase. The objective here is to lower the impact of affected devices and minimize the propagation of the attack.

To our existing solution, as it is being illustrated in Figure 1, we have added a machine learning platform that will receive data from the user and control plane in the Network Layer in which we analyse GPRS Tunnelling Protocol (**GTP**) and Packet Data Convergence Protocol (**PDCP**) traffic [17], allowing us to understand the behaviour of the connected devices.

As to why we consider **GTP** traffic: A subscriber's traffic will differ wildly from that destined for network operators or a network slice dedicated to IoT. Charting a course for **GTP** traffic is usually based on the content of **GTP** messages (**GTP** Information Elements) and also – but not limited to – other aspects like source and destination. A smart GTP routing function can select the right Packet Gateway (**PGW**) or network slice that best suits a specific service. Fortunately, existing technology is capable of harnessing advanced routing, proxy, and security functionalities while being able to access **GTP** Information Elements. Some for example can tap into over 100 types of these including APN, IP address, MS-ISDN, RAT Type, PDN Type (v4/v6), user location info, aggregate max bit rate, and quality of service.

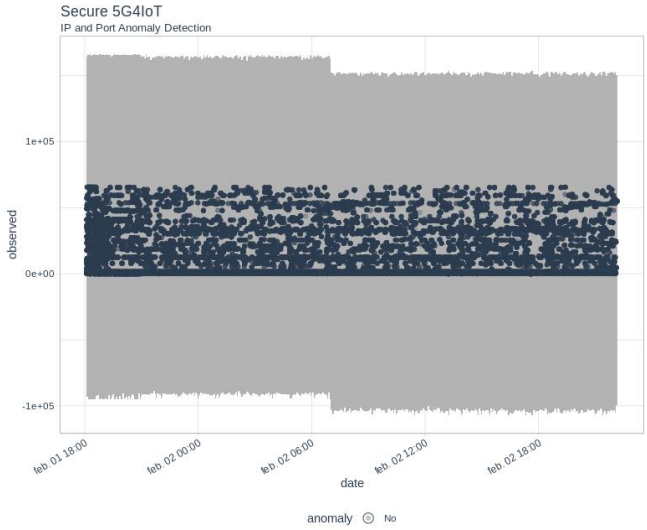

Figure 2. Anomaly Graph representation of normal data traffic (no anomalies detected).

V. IMPLEMENTATION

To support our proposed solution, we have established a proof-of-concept at the Secure 5G4IoT Lab ate the Oslo Metropolitan University, consisting of a 4G/5G mobile network implementation [19] with Identity Management features designed for the IoT paradigm.

The new addition to our solution is the machine learning platform for data processing and analysis. Due to its functions and requirements, the machine has to have better specs such

as two GPUs and more RAM compared to other servers that we have in our implementation. Besides the hardware, the machine is equipped with a machine learning software bundle consisting of tools such as *R Studio* [20], *Kafka* [21], *Spark* [22] and *Jupyter* [23], that will allow us to develop more intricate applications and handle the data traffic in a more efficient way.

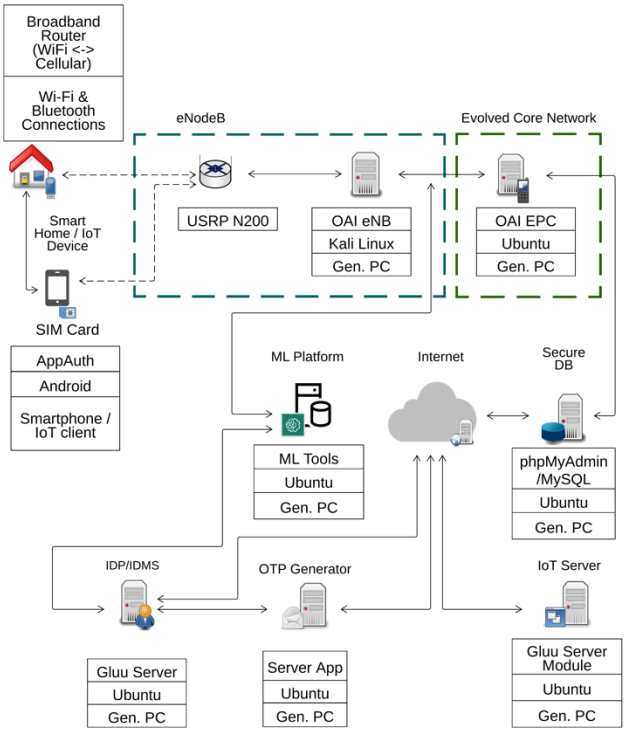

Figure 3. Illustration of the implemented proof of concept.

VI. Future Work

As we established our proof-of-concept and achieved some preliminary results, we see that our proposal is feasible and can be further developed to consider the following aspects:

- **Feature Inclusion:** as we progress with the inclusion of more devices in our solution as to enact more real-life scenarios, there will be a need to include more features to our model and therefore adapt our device profiles. This will allow us to fully extend it as to be able to proper identify most behaviours that devices will have while connected;

- **Model Training:** as more data portraying various types of scenarios becomes available, (which some include attacks and exploits), the model has to be trained as to adapt to all these situations so that its confidence levels are high and reliable at all times;

- **Streamlining/Automation:** as of now the links between the existing solution and its recent addition are purely functional, meaning that a lot of aspects and validations are still made manually. As we progress, with the available software bundle, our platform will be feeded automatically and the data will also be readied by pre-processing methods, so that the anomaly detection model can act efficiently. As anomalies occur, the call to action will eventually be automatized where allowed as to contain the attack in the fastest way possible, as it is intended.

VII. Conclusion

In this work, we've demonstrated through our proposed solution and proof-of-concept a way to improve security to **IoT** devices using the cellular network. By having an identity management system and an identity federation, it will allow to secure connected devices by providing authentication and authorization mechanisms to be used both in the Application and Network layers. Aligned with this, we have a machine learning platform to perform anomaly detection analysis on data traffic, that will allow to minimize the impact of an attack or an exploit as both systems will work together to isolate infected devices.

With further work, this concept will be extended to accommodate more scenarios as we integrate more devices to portray real-life situations.

Acknowledgment

This paper is a result of the H2020 CONCORDIA project (https://www.concordia-h2020.eu) which has received funding from the EU H2020 programme under grant agreement No 830927. The CONCORDIA consortium includes 23 partners from industry and other organizations such as Telenor, Telefonica, Telecom Italia, Ericsson, Siemens, BMW, Airbus, etc. and 23 partners from academia such as CODE, university of Twente, OsloMet, etc.

References

[1] J. S. Kim, S. Lee, and M. Y. Chung, "Time-division random-access scheme based on coverage level for cellular internet-of-things in 3GPP networks," *Pervasive Mob. Comput.*, vol. 44, pp. 45–57, 2018.

[2] Z. Ning, X. Wang, X. Kong, and W. Hou, "A social-aware group formation framework for information diffusion in narrowband internet of things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1527–1538, 2018.

[3] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," *2017 Int. Smart Cities Conf. ISC2 2017*, vol. 00, no. c, 2017.

[4] M. Lenco, "Digital identity as a key enabler for e-government services," *Mob. Connect - GSMA*, pp. 1–8, 2016.

[5] Maliki, T. El, & Seigneur, J. (2007). A Survey of User-centric Identity Management Technologies Requirements. *International Conference on Emerging Security Information Systems and Technologies*, 12–17. http://doi.org/10.1109/SECURWARE.2007.6

[6] D. Van Thanh, I. Jørstad, and D. Van Thuan, "Strong authentication for web services with mobile universal identity," *Lect. Notes Comput.*

Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9228, pp. 27–36, 2015.

[7] IETF Request for Comments: 6749: The OAuth 2.0 Authorization Framework, October 2012

[8] OpenIDConnect:http://openid.net/connect/

[9] 5GPPP Architecture Working Group, "view on 5G architecture," *White Pap.*, no. June, 2019.

[10] H. Khalili *et al.*, "Orchestrator design, service programming and machine learning models ((D4.1)," Feb. 2019. https://doi.org/10.5281/zenodo.2558305

[11] K. Gai, M. Qiu, L. Tao, and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G," *Secur. Commun. Networks*, vol. 9, no. 16, pp. 3049–3058, Nov. 2016. http://doi.wiley.com/10.1002/sec.1224

[12] R. Raina, A. Battle, H. Lee, B. Packer, and A. Y. Ng, "Self-taught learning: Transfer learning from unlabeled data," in *ACM International Conference Proceeding Series*, 2007, vol. 227, pp. 759–766. http://portal.acm.org/citation.cfm?doid=1273496.1273592

[13] Z. Huang, "Extensions to the k-means algorithm for clustering large data sets with categorical values," *Data Min. Knowl. Discov.*, vol. 2, no. 3, pp. 283–304, 1998. http://doi.org/10.1023/A:1009769707641

[14] M. Goldstein and S. Uchida, "A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data," *PLoS One*, vol. 11, no. 4, 2016. https://doi.org/10.1371/journal.pone.0152173

[15] J. Hochenbaum, O. S. Vallis, and A. Kejariwal, "Automatic Anomaly Detection in the Cloud Via Statistical Learning," 2017. http://arxiv.org/abs/1704.07706

[16] B. Santos, B. Dzogovic, B. Feng, V. T. Do, N. Jacot, and T. Van Do, "Enhancing Security of Cellular IoT with Identity Federation," in *Advances in Intelligent Networking and Collaborative Systems*, 2020, pp. 257–268.

[17] L. Ladid and G. Karagiannis, "D3 . 4 : Harmonisation of Standards for 5G Technologies," 2019.

[18] R Language - https://www.r-project.org/, last accessed: November 2019

[19] B. Dzogovic, B. Santos, T. Van Do, B. Feng, T. Van Do, and N. Jacot, "Bringing 5G Into User's Smart Home," *2019 IEEE Intl Conf Dependable, Auton. Secur. Comput. Intl Conf Pervasive Intell. Comput. Intl Conf Cloud Big Data Comput. Intl Conf Cyber Sci. Technol. Congr.*, pp. 782–787, Aug. 2019.

[20] R Studio - https://rstudio.com/, last accessed: November 2019

[21] Apache Kafka - https://kafka.apache.org/, last accessed: November 2019

[22] Apache Spark - https://spark.apache.org/, last accessed: November 2019

[23] Project Jupyter - https://jupyter.org/, last accessed: November 2019