A Dynamic Recommendation-based Trust Scheme for the Smart Grid

Dimitrios Pliatsios*, Panagiotis Sarigiannidis*, George F. Fragulis*, Apostolos Tsiakalos†, Dimitrios Margounakis†
*Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani 50100, Greece
† Sidroco Holdings Ltd, Nicosia 1077, Cyprus
dpliatsios@uowm.gr, psarigiannidis@uowm.gr, gfragulis@uowm.gr, atsiakalos@sidroco.com, dmargoun@sidroco.com

***Abstract*—The integration of the internet of things (IoT) concept into the traditional electricity grid introduces several critical vulnerabilities. Intrusion detection systems (IDSs) can be effective countermeasures against cyberattacks, however, they require considerable computational and storage resources. As IoT-enabled metering devices have limited resources, IDSs cannot efficiently ensure security. To this end, trust evaluation schemes have emerged as promising solutions toward protecting resource-constrained metering devices. In this work, we proposed a trust evaluation scheme for the smart grid, that is based on direct trust evaluation and recommendation. The proposed hierarchical scheme is able to evaluate the trustiness of each metering device without requiring any significant modifications to the already deployed infrastructure. Additionally, the proposed scheme features is dynamic, meaning that it is robust against non-adversarial events that negatively impact the device's trustiness. To validate the performance of the proposed scheme, we carry out network-level simulations and investigate how the various network parameters impact the trust evaluation performance.**

***Index Terms*—cyberattacks, security, smart grid, smart meters, trust management**

I. Introduction

Due to the rapid population growth, the energy demands of the 21st century are exponentially growing [1]. As a result, considerable efforts are being focused on integrating intelligence into the electricity grid. This novel electricity grid, called smart grid, features improved efficiency, increased reliability, and high adaptability to the energy demand. As smart grid evolved, the internet of things (IoT) paradigm has emerged as its main enabler. Through the deployment and interconnection of multiple IoT devices, smart grid can effectively monitor and manage the generation, distribution, and consumption of energy.

The volume of data generated by the smart grid devices is continuously increasing, introducing several scalability, processing, and storage challenges [2]. In this direction, novel technologies, such as Network Function Virtualization (NFV) and Software Defined Networking (SDN), are being incorporated into the smart grid in order to address these scalability challenges [3]. By leveraging these technologies, computation-intensive energy analytics can be placed closer to the consumers.

The electricity grid relied on 'security through obscurity' by operating on isolated networks and proprietary communication protocols. As a result, the cybersecurity considerations of industrial networks were trivial [4]. However, the integration of IoT into the electricity grid has introduced a series of vulnerabilities. As the IoT-based smart grid consists of a multitude of nodes, it features a huge attack surface for an IoT-focused cyber-attack.

To this end, several security countermeasures have been employed [5] to enhance smart grid security, such as intrusion detection systems (IDSs) [6], [7]. However, IDSs rely heavily on previous knowledge of cyberattack patterns or network behavior. Industrial honeypots have emerged as valuable assets towards protecting industrial network devices and discovering new attack patterns for IDSs [8].

Although these security measures can effectively increase smart grid resilience against cyberattacks, they require considerable computational and storage resources. Consequently, they are inefficient in protecting IoT metering devices, due to the limited computational and storage resources of these devices. To address this, trust management has emerged as a promising concept towards protecting devices with limited resources [9]. As a result, various trust management schemes for the smart grid have been proposed [10]–[14]. Particularly, in [10], the authors presented a trust model based on fuzzy logic for detecting malicious selfish nodes that drop packets and investigated non-stable behaviors that affect the model. In [11], the authors leveraged a hierarchical trust score evaluation approach in order to discover and isolate the nodes that participate in a blackhole attack, while in [12] and [13], Velusamy *et al.* combined Bayesian, Dempster-Shafer, Analytical Hierarchy Process, and Fuzzy theory to develop a trusted routing framework for smart grid networks, where each node is able to calculate the neighbors trust and forward the data across a trusted path. Finally, in [14], the authors developed a trust model based on Markov chains and explored the behavior of smart grid devices, in terms of trust level, in presence of different benign and malicious events with varying criticality.

Different from the previous works, we present a layered trust evaluation scheme for smart grid devices based on peer-to-peer interaction for evaluating a device's trust and formulate the corresponding recommendations taking into account the number of interactions. Additionally, motivated by the concept of honeypots [15], we incorporate a new device type that can

978-1-6654-0522-5/21/$31.00 ©2021 IEEE

D. Pliatsios, P. Sarigiannidis, G. Fragulis, A. Tsiakalos, and D. Margounakis, "A Dynamic Recommendation-based Trust Scheme for the Smart Grid," presented at the 2021 IEEE 7th International Conference on Network Softwarization (NetSoft), Jun. 2021. doi: 10.1109/netsoft51509.2021.9492542.

act as a smart grid device, as well as evaluate the trust of other smart grid devices in its proximity. In more detail, the contributions of this paper are as follows:

- We propose a three-layer hierarchical trust architecture that is able to monitor and determine the trust level of each device through the notion of trust value (TV).
- We introduce a novel trust module that mimics the operation and functionalities of a smart meter. It is able to interact with the real smart meters, by requesting routes and forwarding traffic from/to other meters. In addition, TMs communicate with each other in order to verify if their requests have been successfully completed.
- In the top level, the trust coordinator receives the assessments from TMs and determines the TV of each device. To achieve an accurate TV evaluation, the coordinator uses the weighted average approach, where the weights correspond to the number of interactions.
- We leverage a historical decay factor in order to maintain a dynamic TV behavior. As a result, the proposed scheme is robust against temporary device failures due to non-adversarial events, such as power surges, packet collisions, and environmental interference.
- To protect the rest of the network when a device's TV is reduced to a specific value, an alert is broadcasted to the smart grid operator.
- Due to the layered design, the proposed scheme features high scalability. It is able to monitor a massive number of devices through the deployment of additional monitoring modules. In addition, the trust modules can be configured to also operate as honeypots in order to attract adversaries further protecting the rest of devices.
- Finally, by exploiting its layered architecture, the proposed scheme can be deployed in various industrial application scenarios that utilize distributed sensors and actuators.

The rest of the paper is organized as follows: Section II presents the architecture of the proposed scheme, as well as the functionalities of the main components, while Section III presents the evaluation results are presented. Finally, Section IV concludes this work.

II. Proposed Trust Evaluation Scheme

A. Architecture

The three-layered architecture of the proposed scheme is depicted in Fig. 1. The top layer consists of the trust coordinator (TC), which receives the recommendations from the trust modules (TMs) and maintains the TV of each device in the network. The middle layer is composed of N_{TM} TMs, which are deployed throughout the smart grid infrastructure and interact with the smart grid devices, assess their trustiness, and formulate the corresponding recommendations. Each TM can interact with multiple devices in its proximity, as well as communicate with other TMs in order to formulate the recommendations. In this direction, VNF and SDN technologies can be leveraged in order to create a secure and reliable virtual

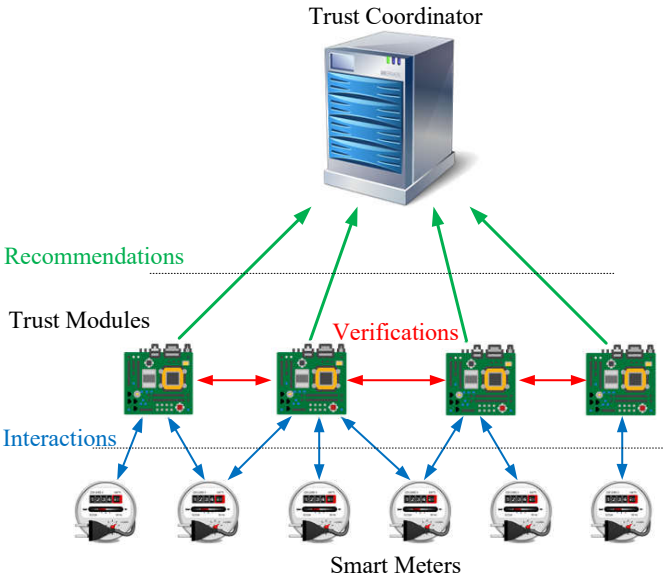


Fig. 1: Hierarchical Architecture

network to be used for the communication requirements of the TMs and the TC. Finally, a number of smart grid devices, denoted by N_{SM} form the bottom layer. These devices carry out metering functionalities that are crucial to the smart grid operation.

B. Direct Trust Recommendation

A TM is a specialized device that is deployed alongside smart meters and mimics their operation. The real metering devices can communicate with the TMs in their proximity and route their data through them, as if they were part of the metering infrastructure. The TM interacts with the metering devices, requesting them to forward data to other TMs. Also, TMs communicate with each other in order to determine whether their data have been forwarded without any issues (e.g., tampering, dropped data, etc.). As a result, through the interactions with metering devices and other TMs, each TM can assess the trustiness of each metering device and formulate the corresponding recommendation to the TC. The operation of TM is summarized in Algorithm 1.

As described in the previous subsection, TMs are responsible for interacting with the smart grid devices and formulating the corresponding recommendations to the TC. Based on the interactions, the direct trust (DT) is determined as

$$\mathrm{DT}_i(j) = \frac{n_{sucess}}{n_{sucess} + n_{fail}}, 1 \leq j \leq N_{SM}, 1 \leq i \leq N_{TM} \quad (1)$$

where i denotes the TM that evaluates the DT of the j-th device, while n_{sucess} and n_{fail} denote the number of successful and unsuccessful interactions, respectively. Based on equation (1), DT is a real number in the range $[0, 1]$, where 0 indicates total distrust and 1 total trust.

After assessing the DT, TM forwards a recommendation to the TC, which consists of the DT value and the total number of interactions, $n_{total} = n_{sucess} + n_{fail}$.

Algorithm 1 Trust Module Operation

Input: $\mathcal{N}_{SM}$: the sets of nodes that the TM interacts with
$\mathcal{N}_{TM}$: the set of TMs that the TM can communicate

while TM running **do**
  Select a random node $\text{N}_i \in \mathcal{N}_{SM}$ and a random TM $\text{TM}_j \in \mathcal{N}_{TM}$
  Request from N_i to forward data to TM_j
  Verify with TM_j if the data have been received correctly
  if Data have been received correctly **then**
    $n_i^{success} = n_i^{success} + 1$
  else
    $n_i^{fail} = n_i^{fail} + 1$
  end if
  if Trust coordinator requests recommendations **then**
    for $i \in \mathcal{N}_{SM}$ **do**
      Send the recommendation DT_i and the total number of interactions $n_i^{total} = n_i^{success} + n_i^{fail}$
    end for
  end if
end while

C. Final Trust Value Evaluation

Algorithm 2 Trust Coordinator Operation

Input: $DT_i(j)$: the recommendations of all nodes from all TMs
$n_{total}(i,j)$: the total number of TMs-nodes interactions
t_{int} the recommendation request interval

while TC running **do**
  Request $DT_i(j)$ and $n_{total}(i,j)$ from TMs
  for $j = 1$ **to** N **do**
    Calculate the temporary $\text{TV}(j)$ using equation (2)
    Calculate the t-th iteration $\text{TV}(j)^{(t)}$ using equation (3)
    if $\text{TV}(j)^{(t)} < \text{TV}_{sense}$ **then**
      Notify the network administrator
    end if
  end for
end while

The TC is responsible for accumulating the recommendations from all TMs and determining the overall TV of the j-th smart meter as

$$\text{TV}(j) = \frac{\sum\limits_{i \in \mathcal{N}_{SM}} n_{total}(i,j)\text{DT}_i(j)}{\sum\limits_{i \in \mathcal{N}_{SM}} n_{total}(i,j)} \tag{2}$$

where $\mathcal{N}_{SM}$ denotes the set that includes the devices that have interacted with the i-th TM.

When the TV of a device is reduced to a specific value an alert is broadcasted to the smart grid operator. This can effectively protect the rest of the network against malicious activities. However, this may lead to a device being falsely isolated, due to non-adversarial events, such as power outages or packet collisions. To this end, we utilize a historical decay concept that enables devices to re-enter the network upon legitimate behavior [16]. Therefore, the TV will be calculated as

$$\text{TV}(j)^{(t)} = (1-\lambda)\text{TV}(j)^{(t)} + \lambda\text{TV}(j)^{(t-1)} \tag{3}$$

where t and $t-1$ are the current and previous TV indexes, respectively, while λ denotes the decay factor and is calculated as

$$\lambda = \frac{\alpha}{1 + e^{-\beta\Delta}} + \gamma \tag{4}$$

where α, β, and γ are the decaying parameters. In particular α controls the impact of the previous TV on the new TV, β controls the impact of the difference between the previous and new TV, and γ is used to enforce the TV in the [0,1] range. Finally, Δ is determined as

$$\Delta = TV(j)^{(t)} - TV(j)^{(t-1)} \tag{5}$$

TABLE I: Simulation Parameters

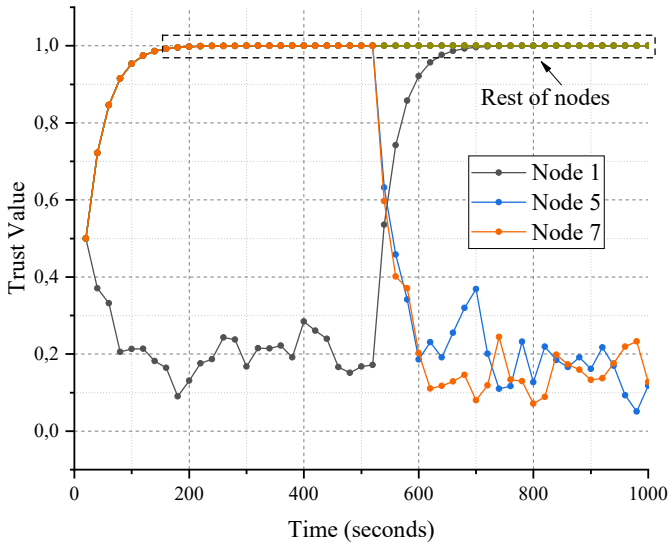
Parameter	Notation	Value
Number of smart meters	N_{SM}	10
Number of TMs	N_{TM}	10
Number of malicious nodes	N_{TM}	1–5
Percent of traffic drop	p_{drop}	80%
Recommendation interval	t_{int}	10, 20, 50, 100 seconds
Initial TV	$\text{TV}^{(0)}$	0.5
Detection sensitivity	TV_{sense}	0.3 – 0.5
Decaying parameters	$\{\alpha, \beta, \gamma\}$	$\{0.1, 0.5, 0.5\}$
Simulation time	T_{sim}	1000 seconds

III. Evaluation

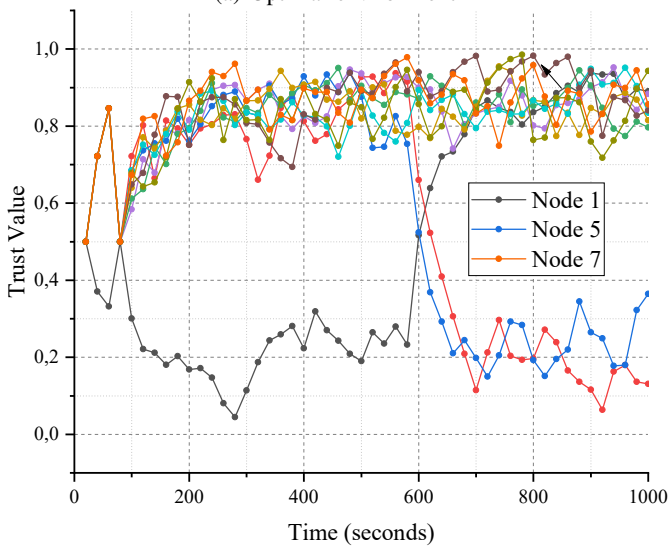
To evaluate the proposed trust scheme, we developed a simulator in Matlab and carried out extensive network-level simulations. In this work, we consider the selfish behavior of a smart meter. Once compromised, a smart grid device can be configured to act as a selfish node that drops packets. The selfish node can either drop all received packets, consisting of both control and data packets, or drop a specific portion of packets, making it harder to distinguish whether packets are dropped due to a compromise or due to heavy network load [17].

The simulation parameters are summarized in Table I. The dropped traffic percentage of selfish nodes is set to 80%. The numbers of smart meters and TMs deployed are 10, while the number of malicious nodes ranges from 1 to 5. The recommendation interval ranges from 10 to 100 seconds. All smart meters are assumed to start with a neutral behavior, thus, the initial TV is set to 0.5, while the detection sensitivity ranges from 0.3 to 0.5. To achieve a rigorous TV update in each iteration, the decaying parameters $\{\alpha, \beta, \gamma\}$ are respectively set to 0.1, 0.5, and 0.5. Finally,the simulation time is set to 1000 seconds.

Figure 2 depicts two scenarios that evaluate how the TVs of the nodes change over time when there are 10 TM and 10 SM. In the first scenario (Fig.2a), an optimal propagation environment is simulated, where there are now wireless propagation



(a) Optimal environment



(b) Suboptimal environemnt due to wireless losses

Fig. 2: Trust value as a function of time when $N_{TM} = 10$ and $N_{SM} = 10$

losses, whereas, in the second scenario (Fig.2b), a propagation environment with data loss due to obstacles is simulated. In both scenarios, node 1 is configured to act as a selfish node for the first half of the simulation, while nodes 5 and 7 have been configured to act as selfish nodes for the second half of the simulation.

Based on the simulation results, node 1 features a low TV in the early seconds and as it begins normal operation, the TV rises. At the same time, node 5 and node 7 start behaving maliciously, and thus, their TV starts decreasing. Therefore, the detection of behavior change, i.e., malicious to benign for node 1 and benign to malicious for nodes 5 and 7, is successfully detected by the proposed trust scheme. Additionally, the proposed scheme enables the quick re-entry of a malicious device after showing a benign behavior.

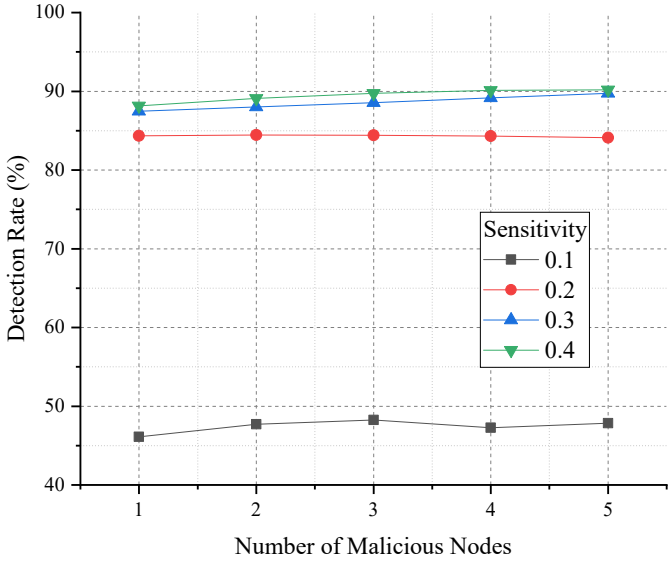


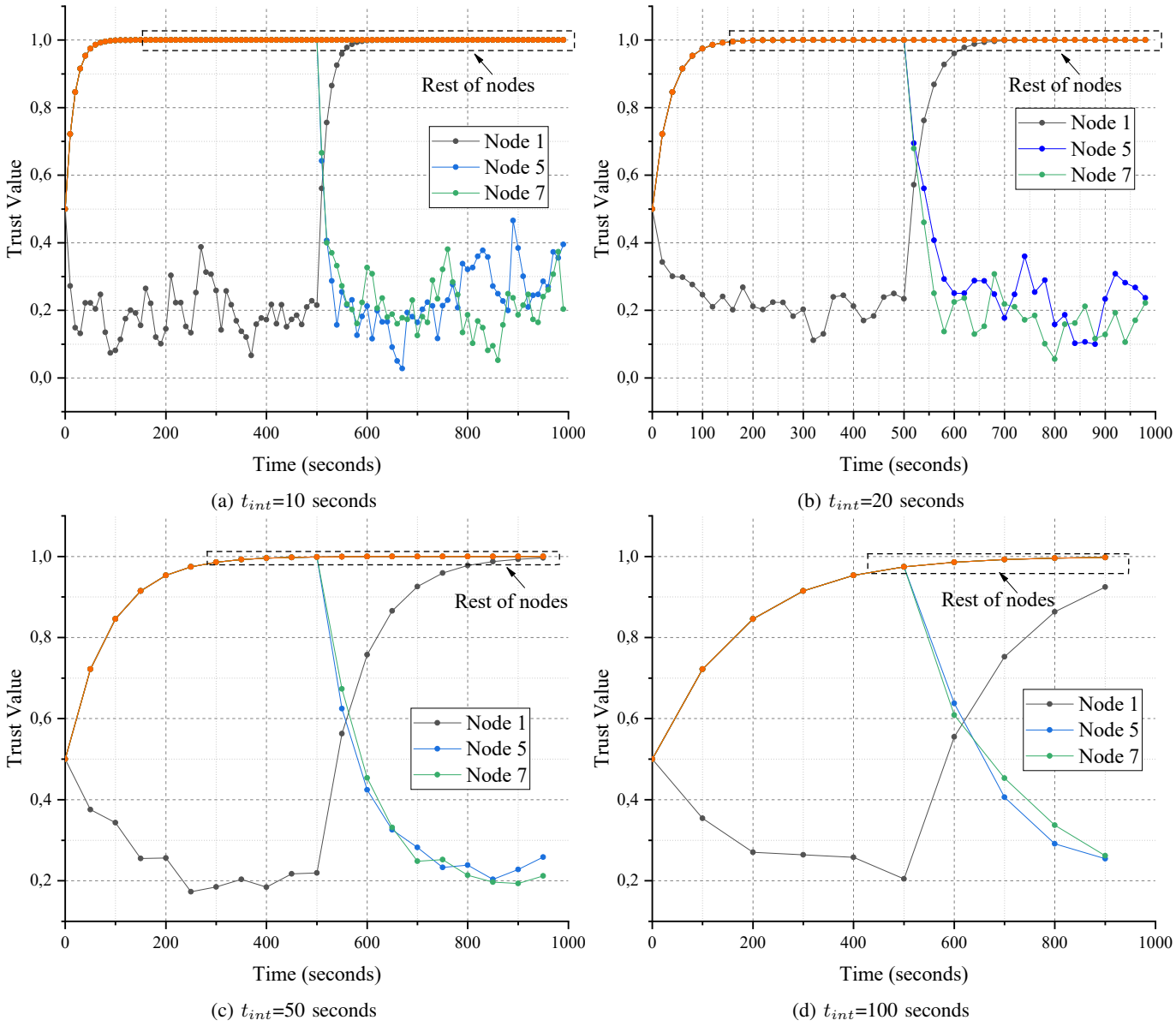
Fig. 3: Detection rate as a function of the number of malicious nodes for various decetion sensitivity

As far as the suboptimal propagation environment is concerned (as depicted in Fig.2b), a similar behavior change for nodes 1, 5, and 7 is observed. Therefore, it can be deduced, that the proposed scheme can successfully detect selfish nodes even in suboptimal propagation environments.

Fig. 3 shows the detection rate of the proposed trust scheme as a function of the number of malicious nodes when the detection sensitivity is 0.1, 0.2, 0.3, 0.4 and the recommendation interval is 20 seconds. It is expected that, when the detection sensitivity is reduced, the detection rate will increase. According to the results, the proposed scheme features a detection around 85-90% when the sensitivity ranges from 0.2 to 0.4. Finally, the number of malicious nodes does not considerably impact the detection rate.

The impact of the recommendation interval on the trust scheme's overall performance in a communication environment without interferences is presented in Fig. 4. Specifically, in Figs. 4a-4d the TC receives recommendations every 10, 20, 50, and 100 seconds. In all four scenarios, node 1 behaves maliciously from the beginning and starts the benign behavior at 500 seconds, while nodes 5 and 7 behave normally and start the malicious behavior (i.e., dropping 80% of the traffic) at 500 seconds.

It is apparent, that in low recommendation intervals (i.e., Fig. 4a and Fig. 4b) the count of TV evaluations for each node is high, contrary to the other cases. Therefore, we can assume that lower recommendation intervals correspond to a more accurate TV evaluation. As a result, the selfish node detection latency is higher when the recommendation interval is high because more time elapses until the next TV evaluation. Therefore, malicious nodes have more time to disrupt the normal network operation. The results indicate that a low recommendation interval can guarantee a low detection time. However, as the recommendation interval is reduced



(a) t_{int}=10 seconds

(b) t_{int}=20 seconds

(c) t_{int}=50 seconds

(d) t_{int}=100 seconds

Fig. 4: Trust value over time for various recommendation intervals

more energy is consumned as the TMs have to submit more recommendations. Based on this remark, we can deduce that the recommendation interval $t_{int} = 20$ seconds offers the best trade-off between the number of recommendations and detection latency.

IV. Conclusion

In this work, we proposed a trust evaluation scheme for the smart grid, that is based on direct trust evaluation and recommendation. The proposed scheme features a three-layered architecture, consisting of the TC in the top layer, the TMs in the middle layer, and the smart meters in the bottom layer. In the proposed architecture, the TMs directly assess the trustiness of each smart meter and send recommendations to the TC. Consequently, the TC receives the recommendations and calculates the TV of each smart meter. To introduce a dynamic trust evaluation and increase the scheme's robustness against non-adversarial events that impact the device trustiness, we integrated a historical decay factor.

The layered architecture can achieve a more accurate evaluation of each smart meter trust, as the TC, being at the top layer, receives multiple recommendations for each smart meter. In addition, the layered architecture can enable high scalability, as additional TMs can be easily deployed to monitor more smart meters. Finally, the TC can know the status of the whole metering infrastructure.

To validate the efficiency of the proposed scheme, we carried out network-level simulation and investigated the impact of non-adversarial events on the TV, such as packet loss due to obstacles and signal losses and the impact of the recom-

mendation interval on the TV. Furthermore, we evaluated the scheme's detection rate as a function of malicious nodes for various detection sensitivity.

As future work, we aim to optimize the deployment of the TMs, as well as their assignment to smart meters, in order to increase the detection accuracy. Additionally, we aim to investigate the tradeoff between the recommendation interval and the detection latency and develop an appropriate optimization solution. Finally, taking into account that the layered architecture of the proposed scheme enables the behavior monitoring of a large number of distributed devices, it suitable for deployment in various Supervisory Control and Data Acquisition (SCADA) applications that utilize distributed sensors and actuators. Consequently, we aim to explore the deployment and configuration of the proposed scheme in additional industrial application scenarios.

ACKNOWLEDGEMENT

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 787011 (SPEAR).

REFERENCES

[1] F. Caputo, B. Buhnova, and L. Walletzký, "Investigating the role of smartness for sustainability: insights from the smart grid domain," *Sustainability Science*, vol. 13, no. 5, pp. 1299–1309, Mar 2018.

[2] C. Tu, X. He, Z. Shuai, and F. Jiang, "Big data issues in smart grid – a review," *Renewable and Sustainable Energy Reviews*, vol. 79, pp. 1099–1107, Nov 2017.

[3] A. Kumari, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and J. J. P. C. Rodrigues, "Fog computing for smart grid systems in the 5g environment: Challenges and solutions," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 47–53, Jun 2019.

[4] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on SCADA systems: Secure protocols, incidents, threats and tactics," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[5] P. I. Radoglou-Grammatikis and P. G. Sarigiannidis, "Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems," *IEEE Access*, vol. 7, pp. 46 595–46 620, 2019.

[6] G. Efstathopoulos, P. R. Grammatikis, P. Sarigiannidis, V. Argyriou, A. Sarigiannidis, K. Stamatakis, M. K. Angelopoulos, and S. K. Athanasopoulos, "Operational data based intrusion detection system for smart grid," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, Sep 2019.

[7] D. Pliatsios, P. Sarigiannidis, K. Psannis, S. K. Goudos, V. Vitsas, and I. Moscholios, "Big data against security threats: The SPEAR intrusion detection system," in *2020 3rd World Symposium on Communication Engineering (WSCE)*. IEEE, Oct 2020.

[8] I. Siniosoglou, G. Efstathopoulos, D. Pliatsios, I. D. Moscholios, A. Sarigiannidis, G. Sakellari, G. Loukas, and P. Sarigiannidis, "NeuralPot: An industrial honeypot implementation based on deep neural networks," in *2020 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, Jul 2020.

[9] I. U. Din, M. Guizani, B.-S. Kim, S. Hassan, and M. K. Khan, "Trust management techniques for the internet of things: A survey," *IEEE Access*, vol. 7, pp. 29 763–29 787, 2019.

[10] A. Alnasser and H. Sun, "A fuzzy logic trust model for secure routing in smart grid networks," *IEEE Access*, vol. 5, pp. 17 896–17 903, 2017.

[11] S. Otoum, B. Kantarci, and H. T. Mouftah, "Hierarchical trust-based black-hole detection in WSN-based smart grid monitoring," in *2017 IEEE International Conference on Communications (ICC)*. IEEE, May 2017.

[12] D. Velusamy and G. K. Pugalendhi, "Fuzzy integrated bayesian dempster–shafer theory to defend cross-layer heterogeneity attacks in communication network of smart grid," *Information Sciences*, vol. 479, pp. 542–566, Apr 2019.

[13] D. Velusamy, G. Pugalendhi, and K. Ramasamy, "A cross-layer trust evaluation protocol for secured routing in communication network of smart grid," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 1, pp. 193–204, Jan 2020.

[14] D. Pliatsios, P. Sarigiannidis, G. Efstathopoulos, A. Sarigiannidis, and A. Tsiakalos, "Trust management in smart grid: A markov trust model," in *2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST)*. IEEE, Sep 2020.

[15] D. Pliatsios, P. Sarigiannidis, T. Liatifis, K. Rompolos, and I. Siniosoglou, "A novel and interactive industrial control system honeypot for critical smart grid infrastructure," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*. IEEE, Sep 2019.

[16] J. Zhao, J. Huang, and N. Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks," *IEEE Access*, vol. 7, pp. 33 859–33 869, 2019.

[17] Y. Chae, L. C. DiPippo, and Y. L. Sun, "Trust management for defending on-off attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 1178–1191, Apr 2015.