Trust Management in Smart Grid: A Markov Trust Model

Dimitrios Pliatsios[§], Panagiotis Sarigiannidis[§*], Georgios Efstathopoulos[†], Antonios Sarigiannidis[‡], and Apostolos Tsiakalos[‡]
[§]Department of Electrical and Computer Engineering, University of Western Macedonia
Kozani, Greece
Email: {dpliatsios, psarigiannidis}@uowm.gr
[†]0INF, Imperial Offices
London, UK, E62JG
Email: george@0inf.com
[‡]Sidroco Holdings ltd.
Limassol, Cyprus
Email: {asarigia, atsiakalos}@sidroco.com

***Abstract*—By leveraging the advancements in Information and Communication Technologies (ICT), Smart Grid (SG) aims to modernize the traditional electric power grid towards efficient distribution and reliable management of energy in the electrical domain. The SG Advanced Metering Infrastructure (AMI) contains numerous smart meters, which are deployed throughout the distribution grid. However, these smart meters are susceptible to cyberthreats that aim to disrupt the normal operation of the SG. Cyberattacks can have various consequences in the smart grid, such as incorrect customer billing or equipment destruction. Therefore, these devices should operate on a trusted basis in order to ensure the availability, confidentiality, and integrity of the metering data. In this paper, we propose a Markov chain trust model that determines the Trust Value (TV) for each AMI device based on its behavior. Finally, numerical computations were carried out in order to investigate the reaction of the proposed model to the behavior changes of a device.**

***Index Terms*—Advanced Metering Infrastructure, Cybersecurity, Markov Model, Smart Grid, Trust Model**

I. Introduction

According to the World Energy Outlook Report, the global energy demand will grow more than 30% by 2040. In addition, concerns are arising regarding the environmental impact of conventional power systems. In order to satisfy this growing demand and address the environmental concerns, radical changes are required to the current energy generation and distribution grid. To this end, the Smart Grid (SG) concept has emerged as a promising solution to address the aforementioned issues [1]. SG leverages the advancements in Information and Communication Technologies (ICT) to deliver a novel power generation and distribution system. SG provides higher energy efficiency, increased reliability, and seamless integration with renewable energy sources. In addition, SG enables the energy stakeholders to gain better insights into the energy market by collecting consumption information and patterns from the customers.

* Panagiotis Sarigiannidis is the corresponding author

Nevertheless, the integration of ICT to the power grid introduces several security threats. SG is vulnerable to cyberattacks that can have a negative impact on consumer privacy as well as the normal operation of the SG. The National Institute of Standards and Technology (NIST) has defined specific security requirements for the SG, namely confidentiality, integrity, authentication, and availability [2].

However, the implementation of effective security mechanisms is challenging due to the low computational capabilities of the SG devices. To this end, several research works have been proposed that aim to ensure the security requirements considering the computational capabilities of the SG devices.

A. Related Work and Contributions

The authors in [3] presented a robust and configurable trust management toolkit that facilitates the operation of SG systems in the presence of malfunctioning components. The toolkit utilizes reputation-based trust over network-flow algorithms to identify untrusted communication components.

A secure key distribution scheme for SG was presented in [4]. An identity-based signature method and an identity-based encryption method are leveraged to develop a novel anonymous key distribution scheme for SG. In the proposed scheme, a SG device can anonymously access services provided by SG operator using a single private key without the need of a trusted anchor during authentication.

The work in [5] described an efficient real-time approach to detect false data injection attacks in SG by exploiting spatial-temporal correlations between the SG components. The efficiency of the approach is demonstrated through realistic simulations based on the US SG.

The authors in [6] presented a lightweight security and privacy-preserving scheme, based on forecasting the electricity demand for a group of houses that are located in the same area. The proposed scheme satisfies the security and privacy requirements with low communication and computational overhead.

Alnasser and Sun [7] proposed a fuzzy logic trust-based model in order to detect untrusted nodes in the SG. The model calculates the node's trust based on three variables (i.e., direct, indirect, and past trust). The authors evaluated the efficiency of the proposed model using a number of cyberattacks.

The authors in [8] integrated honeypots into the SG network as decoys to attract attackers. They analyze the interactions between the attackers and the honeypots in order to derive optimal strategies for both sides. In addition, the authors evaluated the proposed scheme in a simulated SG testbed.

A similar approach was presented in [9]. The authors implement a high interactive honeypot for SG, that is able to emulate a physical ICS device by replicating realistic traffic from the real device. The proposed SG honeypot was evaluated in a realistic demonstration scenario based on a hydropower plant.

In this work, we utilize Markov chains to model the Trust Value (TV) as a security metric of a SG device. The notion of TV is used in various networks, such as peer-to-peer networks [10], wireless sensor networks [11], Multicast Mobile Ad-hoc Networks (MANETs) [12], and vehicular networks [13]. The main contributions of this work are summarized as follows:

- We describe a Markov-based model that can effectively capture the TV change sequence of a SG device. In particular, each TV is represented by a single state in a Markov chain. The states change according to the device behavior.
- We present six events that affect the TV (i.e., the state in the Markov chain) of each device. Specifically, three events correspond to a benign device behavior, while the other three correspond to malicious device behavior. Each of the events has a different impact on the TV/state.
- We analyze the proposed Markov model in order to calculate the probability of the trust state for each SG device and determine the convergence speed.

II. Markov Trust Model for AMI

One of the main components of the SG is the Advanced Metering Infrastructure (AMI). The AMI is a combination of hardware and software technologies that facilitate the collection and management of consumer data [14]. Fig. 1 shows a reference architecture of the AMI. In AMI, multiple smart meters are deployed in the consumer premises (e.g., houses, malls, factories, etc.) in order to collect detailed consumption data. These data are forwarded to a data center for further processing.

AMI devices are susceptible to numerous cyberattacks. For example, an attacker can launch Denial of Service (DoS) attacks against the devices in order to prevent them from their normal operation. Another example is false data injection attacks. After compromising a device, the attacker can inject false data in order to disrupt the operation of the SG or maliciously increase the consumer billing rate.

The notion of TV is used to measure the trust of each AMI device. A central entity, located in the data center, monitors the behavior of the devices and changes the TV accordingly.

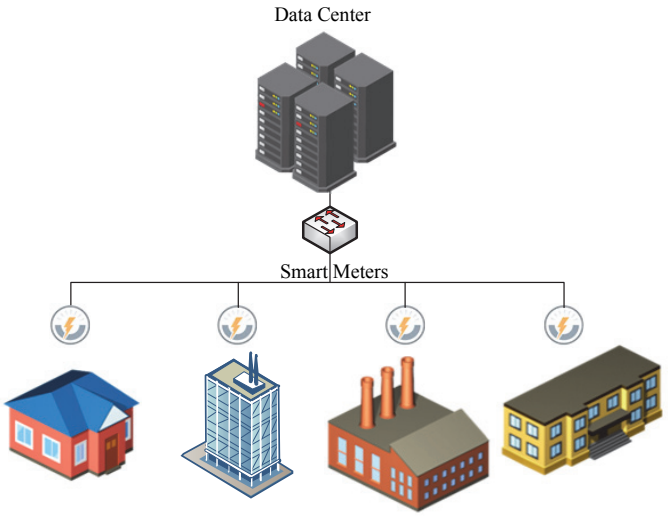

Fig. 1. Advanced Metering Infrastructure Architecture

TABLE I
Event Impact on the TV

Event	TV Change
Normal connection	+1
Abnormal connection	-1
Timely polling response	+2
Delayed polling response	-2
Consumption in the expected range	+3
Consumption out of the expected range	-3

The term $T(i)$ denotes the TV of the i device that changes depending on the device behavior. Similarly to the work in [12], the TV of a device is increased or decreased by 1, 2, and 3 units, respectively. A summary of these events is shown in Table I.

Connection: The device should initiate a connection with the data center by sending a connection request packet. If multiple connection request packets are sent, the connection is considered abnormal and the TV is reduced by 1, otherwise, TV is increased by 1.

Polling: The AMI devices are polled in order to report the consumption data. If the polled device responds within a time limit, the TV is increased by 2, otherwise, it is reduced by 2.

Consumption: If the collected consumption data are in the expected range (e.g., the consumption does not exceed a threshold or it does not differ too much compared to previous values), the TV is increased by 3. Otherwise, the TV is decreased by 3, e.g., in case of device compromise.

The change of TV can be modeled as a Continuous Time Markov Chain (CTMC) [15]. Fig. 2 shows the state diagram of the proposed Markov chain model with various arrival and departure rates. The arrival rates $\lambda_{j,j+k}$ increase the trust state, while the departure rates $\mu_{j,j+k}$ decrease the trust state. Index $j, 0 \leq j \leq J$ denotes the state, while index $k, 1 \leq k \leq 3$ is based on Table I.

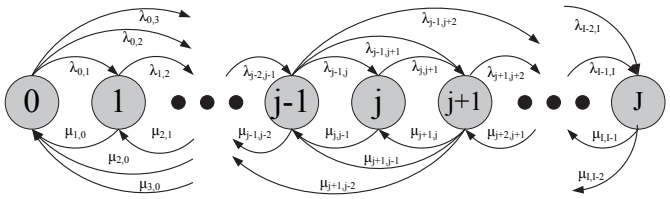

Fig. 2. State diagram of the proposed Markov chain model

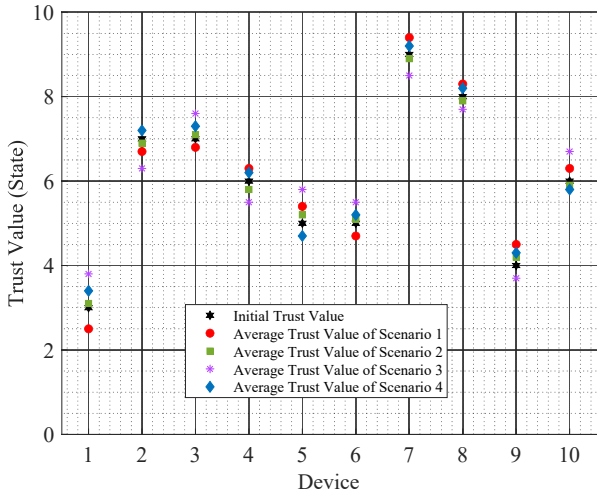

Fig. 3. Average Trust Values

III. Numerical Results

In this section, we present the numerical results of the proposed model regarding the average TVs of the devices as well as the state convergence speed of four scenarios. The system parameters are summarized in Table II. In particular, the number of AMI devices is 10 in all of the scenarios. In scenario 1, the number of trust states is 5, while the arrival and departure rates are exponentially distributed in the range (5,15). In scenario 2, the number of trust states is 5, while the arrival and departure rates λ_1, μ_1 are exponentially distributed in the range (5,15). The rest of arrival and departure rates, based on Table I, are calculated as: $\lambda_2 = 2\lambda_1, \lambda_3 = 3\lambda_1, \mu_2 = 2\mu_1$, and $\mu_3 = 3\mu_1$. Finally, scenarios 3 and 4 have 10 states, while the rest of the parameters are respectively the same with scenarios 1 and 2.

Fig. 3 shows the average TVs of ten devices after 500 transitions. The black stars indicate the initial TV value of each device, while the red circles and green squares indicate the average TVs of each device in scenarios 1 and 2 respectively. Similarly, the purple star and blue diamonds indicate the average TV of the devices in scenarios 3 and 4 respectively. The average TVs of scenarios 2 and 4 are closest to the initial TVs, followed by the average TVs of scenarios 1 and 3. This is expected as scenarios 1 and 2 have fewer states compared to the other two. Overall, it is apparent from both figures, that if a device has a high/low initial TV (i.e., good/bad behavior), it will also have a high/low average TV.

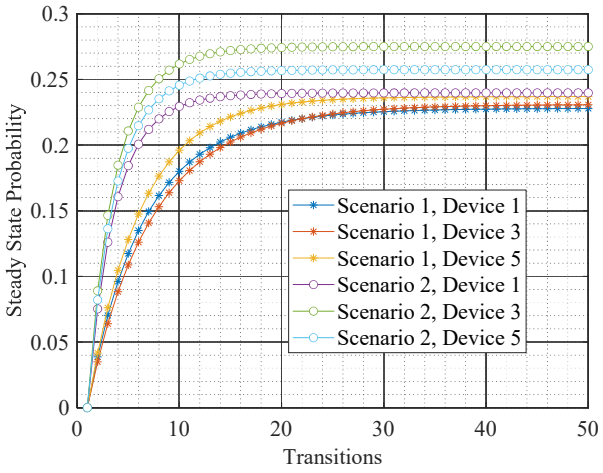

Fig. 4. State Probability Convergence of Scenarios 1 and 2

A comparison between scenarios 1 and 2 in terms of convergence speed is shown in Fig. 4. Specifically, the state probabilities for three (out of five) AMI devices are shown for 50 transitions. Each of the state probabilities starts from 0 and increases its value up to a certain point based on the λ, and μ rates. Particularly, in scenario 1: a) the state probability of device 1 starts from 0 and converges to 0.22 after 35 transitions, b) the state probability of device 3 starts from 0 and converges to 0.23 after 35 transitions, and c) the steady steady probability of device 5 starts from 0 and converges to 0.15 after 30 transitions. Similarly, in scenario 2: a) the state probability of device 1 starts from 0 and converges to 0.24 after 18 transitions, b) the state probability of device 3 starts from 0 and converges to 0.27 after 20 iterations, and c) the steady steady probability of device 5 starts from 0 and converges to 0.26 after 20 iterations.

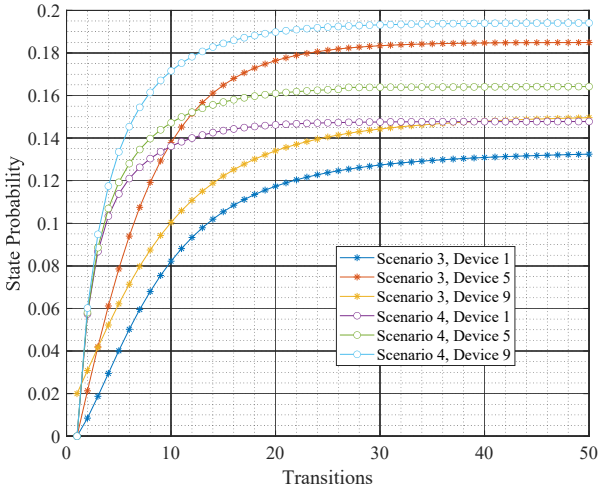

Fig. 5. State Probability Convergence of Scenarios 3 and 4

The convergence speed in scenarios 3 and 4 is shown in Fig. 5. Specifically, the state probabilities for three (out of

TABLE II
SYSTEM PARAMETERS

	Scenario 1	Scenario 2	Scenario 3	Scenario 4
Parameters	**Values**			
Number of AMI devices	10			
Number of trust states	5	5	10	10
λ rates	$\lambda_i = exprnd(5,15), i \in \{1,2,3\}$	$\lambda_1 = exprnd(5,15)$ $\lambda_2 = 2\lambda_1$ $\lambda_3 = 3\lambda_1$	$\lambda_i = exprnd(5,15), i \in \{1,2,3\}$	$\lambda_1 = exprnd(5,15)$ $\lambda_2 = 2\lambda_1$ $\lambda_3 = 3\lambda_1$
μ rates	$\mu_i = exprnd(5,15), i \in \{1,2,3\}$	$\mu_1 = exprnd(5,15)$ $\mu_2 = 2\mu_1$ $\mu_3 = 3\mu_1$	$\mu_i = exprnd(5,15), i \in \{1,2,3\}$	$\mu_1 = exprnd(5,15)$ $\mu_2 = 2\mu_1$ $\mu_3 = 3\mu_1$

ten) AMI devices are shown for 50 transitions. Each of the state probabilities starts from 0 and increases its value up to a certain point based on the λ, and μ rates. Particularly, in scenario 3: a) the state probability of device 1 starts from 0 and converges to 0.13 after 45 transitions, b) the state probability of device 5 starts from 0 and converges to 0.18 after 35 transitions, and c) the steady steady probability of device 9 starts from 0.02 and converges to 0.15 after 40 transitions. Similarly, in scenario 4: a) the state probability of device 1 starts from 0 and converges to 0.15 after 17 transitions, b) the state probability of device 5 starts from 0 and converges to 0.16 after 25 iterations, and c) the steady steady probability of device 9 starts from 0 and converges to 0.19 after 25 iterations.

Based on the previous results, the state probabilities in scenarios 2 and 4 (i.e., $\lambda_1 = exprnd(5,15), \lambda_2 = 2\lambda_1, \lambda_3 = 3\lambda_1$, and $\mu_1 = exprnd(5,15), \mu_2 = 2\mu_1, \mu_3 = 3\mu_1$) converge faster than the ones in scenarios 1 and 3, respectively, due to the arrival and departure rates, being closer to each other, respectively. Moreover, the converged probabilities in scenarios 1 and 2 (i.e., 0.22-0.26) are higher than the respective probabilities in scenarios 3 and 4 (i.e., 0.13-0.19). This is because, in scenarios 1 and 2, the number of states is 5 whereas in scenarios 3 and 4 the number of states is 10. Therefore, the probability of convergence to a specific state increases.

IV. CONCLUSION

In this work, we proposed a Markov chain trust model in order to explore the TV behavior of AMI devices. Moreover, we presented 3 events that increase the TV and 3 additional events that decrease the TV. Based on the analytical results, we conclude that the number of states affects the average TV of each device. Additionally, the arrival and departure rates affect the convergence speed. Consequently, in order to design a high performing trust model, the arrival and departure rates have to be optimally selected. Future extensions of this work involve designing a novel method that optimally selects these rates. In addition, the authors aim to evaluate the proposed trust model in a realistic scenario consisting of physical and simulated testbeds.

ACKNOWLEDGMENT

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

REFERENCES

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—the new and improved power grid: A survey," *IEEE communications surveys & tutorials*, vol. 14, no. 4, pp. 944–980, 2011.

[2] V. Y. Pillitteri and T. L. Brewer, "Guidelines for smart grid cybersecurity," Tech. Rep., 2014.

[3] J. E. Fadul, K. M. Hopkinson, T. R. Andel, and C. A. Sheffield, "A Trust-Management Toolkit for Smart-Grid Protection Systems," *IEEE Transactions on Power Delivery*, vol. 29, no. 4, pp. 1768–1779, 2013.

[4] J.-L. Tsai and N.-W. Lo, "Secure Anonymous Key Distribution Scheme for Smart Grid," *IEEE transactions on smart grid*, vol. 7, no. 2, pp. 906–914, 2015.

[5] P.-Y. Chen, S. Yang, J. A. McCann, J. Lin, and X. Yang, "Detection of false data injection attacks in smart-grid systems," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 206–213, 2015.

[6] A. Abdallah and X. Shen, "Lightweight Security and Privacy Preserving scheme for smart Grid Customer-side Networks," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1064–1074, 2015.

[7] 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.

[8] Z. Ni and S. Paul, "A multistage game in smart grid security: A reinforcement learning solution," *IEEE transactions on neural networks and learning systems*, vol. 30, no. 9, pp. 2684–2695, 2019.

[9] 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, 2019, pp. 1–6.

[10] X. Li, Q. Gao, L. Wu, X. Sun, and S. Deng, "Enhaneigen: A new comprehensive trust model for peer-to-peer network," in *Chinese Intelligent Automation Conference*. Springer, 2017, pp. 105–114.

[11] M. Singh, A. R. Sardar, R. R. Sahoo, K. Majumder, S. Ray, and S. K. Sarkar, "Lightweight trust model for clustered wsn," in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*. Springer, 2015, pp. 765–773.

[12] B.-J. Chang, S.-L. Kuo, Y.-H. Liang, and D.-Y. Wang, "Markov chain-based trust model for analyzing trust value in distributed multicasting mobile ad hoc networks," in *2008 IEEE Asia-Pacific Services Computing Conference*. IEEE, 2008, pp. 156–161.

[13] Z. Wei, F. R. Yu, and A. Boukerche, "Trust based security enhancements for vehicular ad hocnetworks," in *Proceedings of the fourth ACM international symposium on Development and analysis of intelligent vehicular networks and applications*. ACM, 2014, pp. 103–109.

[14] R. R. Mohassel, A. S. Fung, F. Mohammadi, and K. Raahemifar, "A survey on advanced metering infrastructure and its application in smart grids," in *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*. IEEE, 2014, pp. 1–8.

[15] M. Hajiaghayi, B. Kirkpatrick, L. Wang, and A. Bouchard-Côté, "Efficient continuous-time markov chain estimation," in *International Conference on Machine Learning*, 2014, pp. 638–646.