2024

# Trust Model Utilization for Energy Grid Communication

N. Sonali Fernando
*Portland State University*, narmada@pdx.edu

John M. Acken
*Portland State University*, john.acken@pdx.edu

Robert B. Bass
*Portland State University*, robert.bass@pdx.edu

# Trust Model Utilization for Energy Grid Communication

N. Sonali Fernando, John M. Acken, Robert B. Bass
*Department of Electrical and Computer Engineering*
Portland State University
Portland, Oregon, USA
narmada@pdx.edu

*Abstract*—The internet information that is used by the Energy Grid of Things requires both preventative security measures as well as surveillance measures. The preventative security measures include certificates, encryption, and all of the basic security protocols as defined by published standards. The surveillance measures include monitoring information flow activities and evaluating these messages for indications of potential security attacks. We describe in this paper the utilization of a Distributed Trust Model that was developed specifically for monitoring communication within an Energy Grid of Things. The goal for the Distributed Trust Models is to provide a level of aggregate trust that a Distributed Energy Resource Management System can meet its grid service obligations, as opposed to a detailed individual Distributed Energy Resources assessment.

*Index Terms*—Energy Grid of Things, Smart Grid Security, Distributed Trust Model, Distributed Energy Resourcess, Distributed Energy Resource Management System

## I. INTRODUCTION

In order to aggreagte and schedule Distributed Energy Resourcess (DERs), a two-way communication system between energy consumers and energy service providers is provided in an Energy Grid of Things (EGoT) [1]. Any communication system that uses internet protocols is susceptible to many information security vulnerabilities. Energy consumer participation in any internet communication, including an EGoT, encounters privacy and security concerns [2]. When these concerns are addressed openly and properly, then the general public is more inclined to participate in grid service programs, such as demand response [3], [4]. Consumer privacy can be protected in an implementation that does not track individual behavior because the goal for a Distributed Trust Model (DTM) system is to provide a level of aggregate trust that a Distributed Energy Resource Management System (DERMS) can meet grid service obligations, rather than a detailed assessment of individual DERs. For any system that supports sustainable energy distribution the security and trust must be maintained and the DTM contributes to that security and trust. The internet information that is exchanges within an EGoT requires both preventative security measures as well as surveillance measures. Preventative security measures include certificates, encryption, and all of the basic security protocols as defined by published standards. Surveillance measures include monitoring

information flow activities and evaluating these messages for indications of potential security attacks.

The first step of preventative security measures to participate in grid services is for the consumer to follow the registration process defined by a Grid Operator (GO), which results in information security certificates for messages. The registration process abides by the standard protocol [5]. For the preventative security measures, this paper references the IEEE 2030.5 Smart Energy Profile 2.0 (SEP) protocol as the standard that sets security and communication requirements between a Grid Service Provider (GSP) and DERs. For the surveillance measures, this manuscript describes an additional layer of security, specifically the DTM, which augments the security implemented by the SEP.

SEP specifies the following security measurements: Hypertext Transfer Protocol Secure (HTTPS); Access Control Lists (ACLs); and registration lists for authorization. Transport Layer Security (TLS) uses mutual authentication when establishing communication between the server and the client [6]. For encryption, TLS uses Advanced Encryption Standard Cipher Block Chaining - Message Authentication Code (AES-CCM) and requires client-server authentication before establishing a communication channel for message exchange [6]. Even with the preventative security measurements specified by SEP, there is still uncertainty and risk associated with messages and entities in a communication network, and hence there is a need for a monitoring or surveillance DTM system to augment the preventative information security measures.

Rahman and Hailes highlighted a significant security gap in network communication, showing that despite authentication, encryption, and implementation access control (basically preventative security measures), one can not be sure if the correct party provided the encrypted message, even if they provided all the credentials to proceed with a secure communication [7]. Our research adds the idea that even if the correct party does the authentication, there is no way to confirm they are not malicious.

The survey by Kim et al. mentions the current security research and resolutions of a EGoT are about securing wireless communication between electric vehicles and charging stations [8]. Additionally, EGoT communication networks are
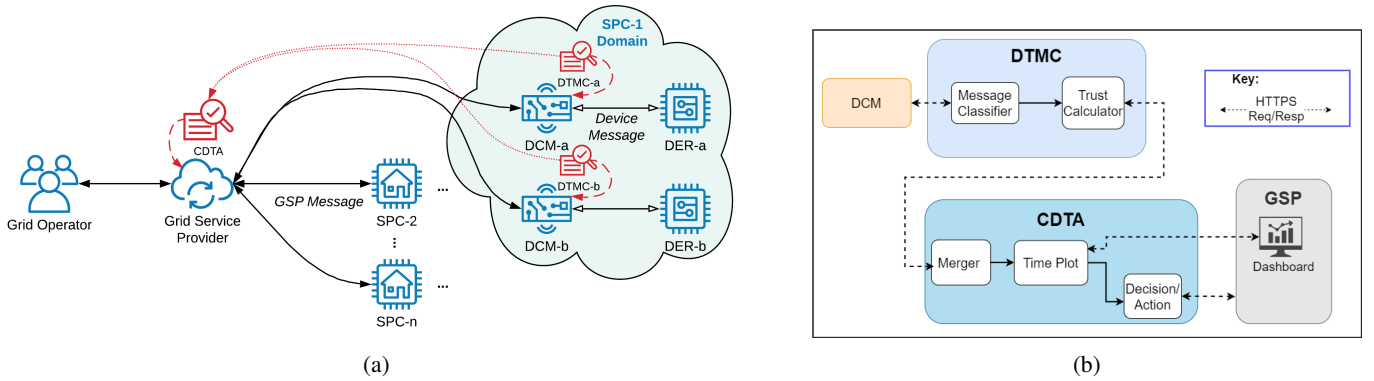
Fig. 1: DTM-EGoT integration. (a) Integration of DTM into the EGoT system. (b) The DTM System described in this paper.

vulnerable to Advanced Persistent Threats (APT) attacks [9]. A DTM can observe for APT when small attacks are conducted within an EGoT communication system. Our DTM system actively monitors EGoT network communication for early detection of abnormalities and potential attacks, and it reports abnormalities to appropriate authorities. A DTM system analyzes the overall trustworthiness of EGoT network communication.

To address the existing security concerns, the Power Engineering Group at Portland State University designed and implemented a DTM system, shown in Figure 1a and Figure 1b [10] [11]. This DTM system consists of two main components, many Distributed Trust Model Clients (DTMCs) and a Central Distributed Trust Aggregator (CDTA). The DTMCs are located at customer homes where they check for abnormalities in the communication path between DERs and the GSP. The second component is the CDTA, a central server that collects and analyzes trust data reported by the DTMCs. The CDTA creates a dashboard to show various trends in trust metrics. Based upon security objectives for a particular electric power system, the CDTA creates diagnostic alert messages that point to potential security threats and has the flexibility to add more detection features or adjust metric value threshold to identify additional attacks.

A unique characteristic of our DTM system is that it is designed specifically for EGoT network communication that follows the SEP messaging scheme. Specifically, the DTMs monitor the header data within SEP messages. However, the design is sufficiently flexible to abide by other protocols such as OpenADR, Consumer Technology Association (CTA)-2045, DNP3 (IEEE 1815), and SunSpec Modbus, all of which are used by utilities to manage DERs [12].

In this paper, section II presents an overview of the architecture of the DTM, followed by the implementation of the DTM communication. Section III provides more detail on the trust equations and the Metric Vector of Trust (MVoT) equations. Section IV describes the category specifics for the DTM communication via the dashboard and messaging scheme. Section V describes example message decisions and how the hypothesis testing procedure is applied for determining

threshold values that trigger when to send alerts. A glossary of terms may be found in section VII.

## II. DTM ARCHITECTURE AND COMMUNICATION

A detailed representation of the DTM system and its communication pathways is shown in Figure 2. A Distributed Control Module (DCM) serves as a gateway between DERs and a GSP, which operates a DERMS server. A DCMs provides encapsulated header information to a DTMC of all messages exchanged between itself, the DER and the DERMS. The DCM forwards these encapsulated messages to the DTMC. The DTMC message classifier then parses and classifies these messages. It then generates new MVoTs based on the classified messages, which it then forwards to the CDTA.

DTMCs have two main tasks. After receiving message packets from their respective DCMs, DTMs classify messages as *expected*, *unexpected*, *indeterminate*, *error*, or *none*. The classified messages are then sent to a trust calculator along with the initiating actor's name, message-sent time, and transit time. Then, the DTMCs conducts trust calculation of incoming messages. New trust values are calculated using existing MVoT data and the provided message classification information. The MVoT is described in the next section.

The CDTA aggregates the trust data sent by all DTMCs. It then organizes the data into MVoT categories to accommodate dashboard plotting and alerts of abnormal activities for authorities, such as the GSP. The GSP dashboard provides a graphical view of the aggregate MVoT data, such as the trust score, distrust score, and message communication frequency. A separate analysis tool uses the MVoT data to provide a statistical analysis of threshold settings using hypothesis testing.

When designing the DTM system, we ensure that the security applied to the network communication between DTM components over the network is secure. Hence, we implement the SEP security requirement to enable HTTPS. HTTPS network communication is enabled along three pathways: one between the DCM and the DTMC server, another between the DTMC client and the CDTA server, and the third between the CDTA and the GSP.
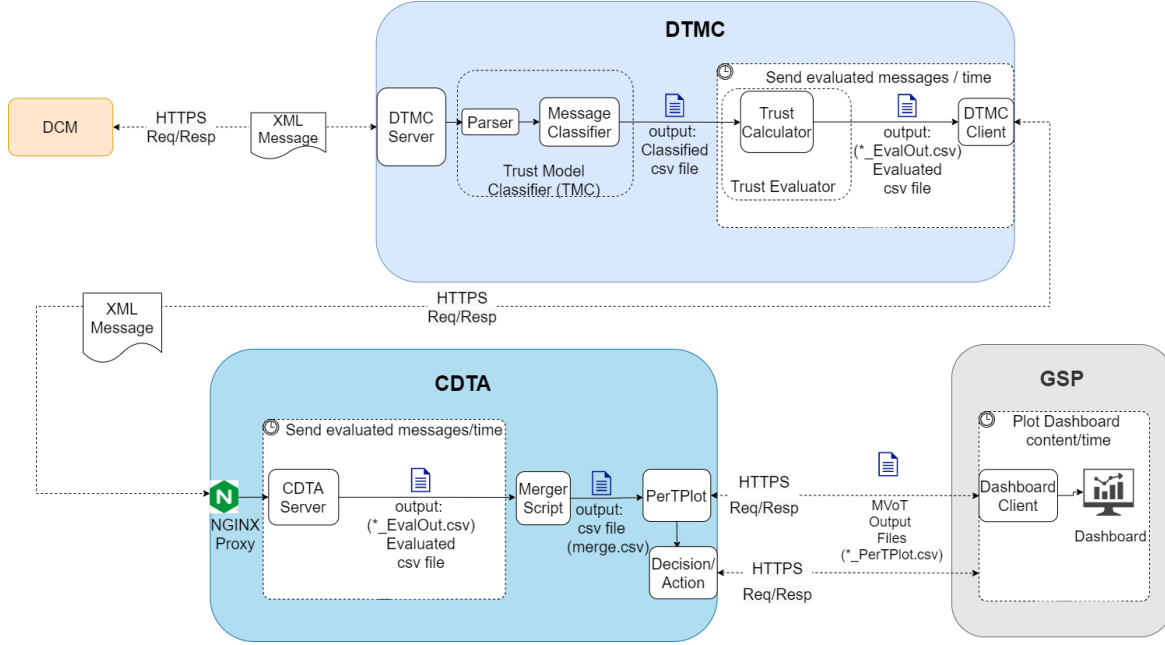
Fig. 2: Detailed representation of the DTM System described in this paper

## III. MVoT Example Equations

Fernando et al. described the MVoT variables and their corresponding equations [13] as listed in Table 1. Notice that many existing trust models arrive at a single score for trust, our DTM has multiple measures for evaluating trust. A single score might hide a recent flurry of unexpected messages over a large past number of expected messages. similarly, an overall score might miss a change in the rate of messages. Also, one must distinguish between overall trust form the specific distrust. The following two examples describe calculating two of the MVoTs.

| Item | Variable | Keyword |
|------|----------|---------|
| 1 | TS | Trust Score |
| 2 | DS | Distrust Score |
| 3 | C | Certainty |
| 4 | CExMsg | Count Of Expected Messages |
| 5 | CUnMsg | Count Of Unexpected Messages |
| 6 | TotMsg | Total Number Of Messages |
| 7 | Time_Stmp | Time of the Last Message Received |
| 8 | Regstr_Time | Registration Date (Unix Time) |
| 9 | ComFreq | Frequency of Communication |
| 10 | TX_Tme | Measured Transit Time |
| 11 | Avg_TX_Tme | Average transaction Time |
| 12 | TSLC | Time Since Last Communication |
| 13 | SDTT | Standard Deviation Of Txn Time |
| 14 | RFC | Relative Factor of Certainty |
| 15 | T_Out | Count Of Timeouts |
| 16 | C_Alrt | Count Of Alerts |

TABLE I: Table providing a list of MVoT variables and the corresponding definitions used in this research

**Trust Score($TS$):** Overall trust score for each actor

$$TS = [CExMSG - (\alpha \times CUnMSG)] \times C \quad (1)$$

**Distrust Score($DS$):** Distrust score for each actor

$$DS = CUnMSG \times C \quad (2)$$

$CExMSG$ represents the count of messages that are classified as expected. $CUnMSG$ represents the count of unexpected messages. $\alpha$ is a weight that determines the relative influence of $CUnMSG$ relative to $CExMSG$ to be set as the GSP observes the DTM during operation. $C$ is the certainty factor based on the amount of data that has been collected.

## IV. DTM Dashboard and Messaging

The DTM dashboard provides the overall health of the EGoT network communication by displaying graphs of MVoT variable behaviors over time. Figure 3 shows a sample dashboard of the DTM system. In our implementation of the dashboard, we provided flexibility to display a selective number of MVoT variable plots. Figure 3 shows how the MVoT plots, such as trust score over time, are critical plots for authorities who want to know the overall health of their EGoT system. The trust score versus time plot shows if there are increasing or decreasing trends in trust. Additionally, the graphical representation of distrust score versus time presents the trend in the mistrust of the system. This enables the observer to understand how many mistrust-worthy incidents are happening within the EGoT network communication, independent of trustworthy incidents. The dashboard can be expanded to include more MVoT variables.

## V. Setting Thresholds for Messages and Alerts

Setting alert thresholds is critical to the DTM system. We developed a hypothesis testing tool to analyze the MVoT calculations of the grid and help authorities, such as a GSP, determine the tolerance level of abnormalities reported by the
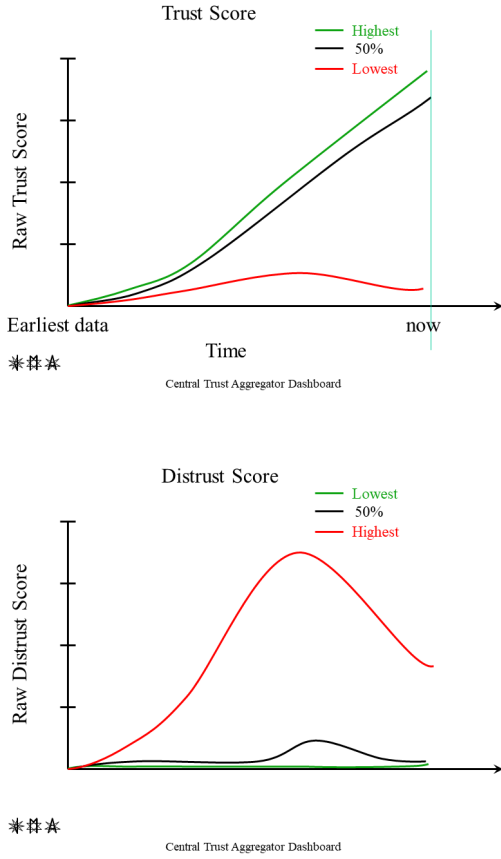
Fig. 3: The DTM dashboard showing the MVoT value trend over time.

DTM system. This feature ensures authorities are not alerted for each incident of MVoT abnormality of just one or a few actors. Instead, the authority can set the tolerance level, and once the set threshold is passed, DTM system sends alerts reporting the specific abnormality trend. A count threshold is a settable number that tells the tolerance for the count of actors with abnormal MVoT values threshold. A value threshold is a settable number used to determine if a MVoT variable value is abnormal when compared to the threshold. A message is sent or an alert raised when the count of entities exceeding the related value threshold exceeds the specified count threshold. Equations 3 and 4 are used to calculate False Positive Rate (FPR) and the False Negative Rate (FNR), which are used to determine thresholds.

$$FPR = \frac{FP}{(FP + TN)} \tag{3}$$

$$FNR = \frac{FN}{(FN + TP)} \tag{4}$$

In these equations, False Positive (FP) is the count of false positive, True Positive (TP) is true positive, False Negative (FN) is false negative, and True Negative (TN) is true negative.

The plot in Figure 4 shows the FP and TP as a function of varying the threshold. Equal Error Rate (EER) is the point where these two lines intercept. The significance of EER is the balancing point where the rate of sending false alerts and failing to send alerts are equal. The hypothesis test tool provides the GSP with a visual representation that helps decide to send too many alerts or hold off until a significantly large amount of abnormalities are present before alerting the GSP.
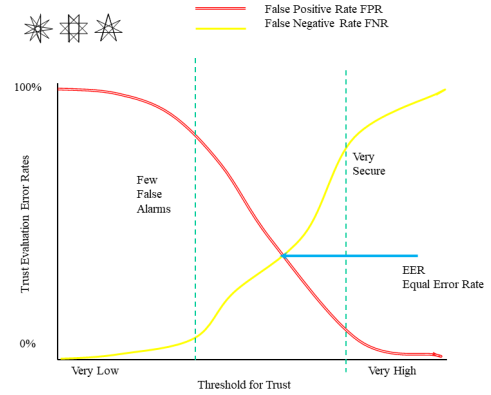


Fig. 4: Effect of Trust Threshold settings.

Once these thresholds are determined and provided, the DTM uses these values to determine when to send alerts. The hypothesis test tool is set to analyze all the MVoT values and help an authority decide on the threshold for each. The FPR, and the FNR are used by the authority to adjust thresholds for the MVoT levels that trigger messages. Lower thresholds will mean more messages and increased false alarms; higher thresholds will mean fewer messages and increased missed alarms. Initially, the DTM will set the thresholds for an equal error rate to balance the FPR and the FNR. It is up to the authority to evaluate the most effective levels for their specific situation. Examples of alert messages sent from the DTM-System to the GSP:

- "Excessive time since last communication from GSP"
- "Excessive time since last communication from DER"
- "Trust is low for GSP"
- "Communication rate is low from GSP"

## VI. Summary and Conclusions

This paper presents implementing and evaluating a distributed trust model to provide evaluation of message trust for the EGoT. Because the system has not been widely implemented, real world experiments will wait for the time when more systems are in place. The DTM calculates a local MVoT which is communicated to the CDTA. The CDTA aggregates all of the DCM MVoTs and based upon count and value thresholds decides whether to send alerts EGoT participants that potential communication attacks may occur. The method to set and adjust thresholds for sending these messages is described. The idea is that trust monitoring can

provide information protection against and early detection of unforeseen attacks, which is a requirement for a sustainable energy grid.

## VII. GLOSSARY

**ACL**     Access Control List
**AES-CCM**   Advanced Encryption Standard Cipher Block Chaining - Message Authentication Code
**APT**     Advanced Persistent Threats
**CDF**     Cumulative Distribution Function
**CDTA**    Central Distributed Trust Aggregator
**CSV**     Comma-Separated Values
**CTA**     Consumer Technology Association
**DCM**     Distributed Control Module
**DER**     Distributed Energy Resources
**DERMS**  Distributed Energy Resource Management System
**DS**      Distrust Score
**DTM**     Distributed Trust Model
**DTMC**    Distributed Trust Model Client
**EER**     Equal Error Rate
**EGoT**    Energy Grid of Things
**FNR**     False Negative Rate
**FPR**     False Positive Rate
**GO**      Grid Operator
**GSP**     Grid Service Provider
**HTTPS**   Hypertext Transfer Protocol Secure
**MVoT**    Metric Vector of Trust
**SPC**     Service Provisioning Customer
**TS**      Trust Score
**TSLC**    Time Since Last Communication

## REFERENCES

[1] S. Widergren, R. Melton, A. Khandekar, B. Nordman, and M. Knight, "The Plug-and-Play Electricity Era: Interoperability to Integrate Anything, Anywhere, Anytime," *IEEE Power and Energy Magazine*, vol. 17, no. 5, pp. 47–58, 2019.

[2] T. Slay, J. M. Acken, and R. B. Bass, "Incentivizing distributed energy resource participation in grid services," in *2022 IEEE Conference on Technologies for Sustainability (SusTech)*, 2022, pp. 86–91.

[3] M. Obi, C. Metzger, E. Mayhorn, T. Ashley, and W. Hunt, "Nontargeted vs. Targeted vs. Smart Load Shifting Using Heat Pump Water Heaters," *Energies*, vol. 14, no. 22, p. 7574, 11 2021.

[4] K. Marnell, C. Eustis, and R. B. Bass, "Resource Study of Large-Scale Electric Water Heater Aggregation," *IEEE Open Access Journal of Power and Energy*, vol. 7, pp. 82–90, 2020.

[5] IEEE Common Smart Inverter Profile Working Group, "Common Smart Inverter Profile: IEEE 2030.5 Implementation Guide for Smart Inverters," IEEE, Tech. Rep., 2018.

[6] "IEEE Standard for Smart Energy Profile Application Protocol," *IEEE Std 2030.5-2018*, pp. 1–361, 2018.

[7] A. Abdui-Rahman, S. Hailes, and S. Hailes, "A Distributed Trust Model," in *New security paradigms*, 1997, pp. 18–60.

[8] Y. Kim, S. Hakak, and A. Ghorbani, "Smart grid security: Attacks and defence techniques," pp. 102–123, 2023.

[9] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," *Internet of Things*, vol. 14, p. 100111, 2021.

[10] N. S. Fernando, J. M. Acken, and R. B. Bass, "Developing a Distributed Trust Model for Distributed Energy Resources," in *2021 IEEE Conference on Technologies for Sustainability (SusTech)*, 2021, pp. 1–6.

[11] M. Alsaid., N. Bulusu., A. Bargouti., N. S. Fernando., J. M. Acken., T. Slay., and R. B. Bass., "Privacy-preserving Information Security for the Energy Grid of Things," in *Proceedings of the 11th International Conference on Smart Cities and Green ICT Systems - SMARTGREENS*. SciTePress, 2022, pp. 110–116.

[12] M. Obi, T. Slay, and R. Bass, "Distributed energy resource aggregation using customer-owned equipment: A review of literature and standards," *Energy Reports*, vol. 6, pp. 2358–2369, 2020.

[13] N. S. Fernando, Z. Zeng, J. M. Acken, and R. B. Bass, "Trust Model System for the Energy Grid of Things Network Communications," in *2023 IEEE Conference on Technologies for Sustainability (SusTech)*. IEEE, 4 2023, pp. 280–287.