

Smart Grid Topology and Error Detection in Smart Meter Networks using CRC

**Vijitha Ananthi J.¹, Vasantha Lakshmi S.², Manisha N.³,
Harika A.⁴, Amrutha M.⁵**

Department of Computer Science, Vignan's Foundation for Science, Technology & Research, Andhra Pradesh, India.

E-mail: ¹jva_cse@vignan.ac.in, ²vs4676914@gmail.com, ³manishanadendla8888@gmail.com, ⁴atukuriharika2@gmail.com, ⁵amrutha0411@gmail.com

Abstract

In smart grid infrastructure, where Smart Meters continuously send usage data to central servers for invoicing, monitoring, and optimization, data transmission reliability is crucial. However, transmission mistakes brought on by noise, interference, and signal attenuation can impair system performance. In this study, the Cyclic Redundancy Check (CRC) is used and tested as an error detection method in Smart Meter communication networks. In comparison to conventional parity approaches, CRC offers greater safety by using polynomial division to identify single-bit and burst mistakes with high accuracy. To investigate the operational efficacy, bandwidth effect, and error detection properties of CRC, a smart grid network was simulated using Cisco Packet Tracer. These findings confirm that CRC is a cost-effective, scalable, and safe method for ensuring dependable communication in wide-area smart grid configurations.

Keywords: Smart Grids, Smart Meter, Cyclic Redundancy Check (CRC), Generator Polynomial, Error Detection, Band- width Overhead, Retransmission.

1. Introduction

By the modernization of the electric power grid, the grids were transformed into smart grids, a technology that employs advanced communication technology and smart control methods to support efficiency, reliability, and sustainability. The focal point of such systems, the SmartMeter, offers real-time electricity usage in an effort to enable two-way communication between electricity consumers and suppliers. The information is highly

essential for load management, defect detection, dynamic pricing, and demand forecasts. Several challenges are, however, bound to limit quality information transfer in the smart grid networks such as electromagnetic interference, signal loss, and channel noise. Interference is likely to contaminate the data or cause bit errors during transmission, impacting energy control, system stability, and correct billing. In order to counteract such effects, strict error detecting processes must be applied to guarantee data integrity in transit.

The Cyclic Redundancy Check, or CRC, is likely the most general error-checking technique employed in communications. CRC performs very well in single-bit and burst error detection, which is most prevalent when data is transmitted, through polynomial-based division to create and verify checksums. CRC is better to previous techniques like parity checks due to its superior fault-detecting characteristics and greater reliability at a lower cost of computation. This study mirrors the topology of the smart grid network and simulates Smart Meter communication under Cisco Packet Tracer. It attempts to authenticate whether the error-detecting feature of CRC is reliable, its bandwidth effectiveness, and how it can be applied to improve secure communication for highly distributed smart grid nodes. The outcome confirms that CRC can provide trustworthiness, scalability, and energy efficiency to high-scale smart grid networks.

2. Related Work

The rapid integration of smart meters and advanced measurement infrastructure has enabled new methods for topology identification, monitoring, and fault detection in modern power distribution networks. Flynn et al. [1] proposed an improved algorithm leveraging smart meter data to enhance topology identification accuracy and enable real-time fault detection, significantly improving reliability in distribution systems. Expanding on this, Pengwah et al. [2] addressed the challenge of incomplete data by developing a topology identification framework capable of operating under partial smart meter coverage, thereby enhancing practical deployability in mixed-infrastructure environments. Earlier work by the same authors [3] focused on radial distribution networks, where smart meter data was used to reconstruct topological structures with high accuracy and scalability. Complementing these approaches, Liu and Huang [4] investigated error estimation in smart meter measurements, emphasizing the importance of correcting metering inaccuracies for reliable topological modeling in low-

voltage systems. Wei et al. [5] contributed an online topology monitoring method that minimizes communication requirements between meters, optimizing both data bandwidth and computational efficiency. Similarly, Soltani and Khorsand [6] integrated micro-PMU and smart meter data for real-time topology detection and state estimation, demonstrating improved responsiveness and precision. Srinivas and Wu [7] extended this hybrid measurement approach to jointly estimate both topology and electrical parameters, further strengthening system observability. From a data integrity perspective, Urrea et al. [8] enhanced smart metering reliability through error detection and correction using the Modbus-RTU protocol, which is vital for high-speed, noise-resilient communication. Abdelkader and Benidris [9] focused on topology error detection within the context of defensive islanding, highlighting the role of accurate network structure awareness in maintaining grid resilience during disturbances. Finally, Qian et al. [10] proposed a topology identification technique suitable for primary distribution networks with sparse smart meter data, offering an adaptable solution for developing grid infrastructures. Collectively, these studies demonstrate significant progress toward intelligent, data-driven topology identification systems that combine smart metering, advanced algorithms, and hybrid sensing to achieve resilient, real-time distribution network management.

3. Research Gap and Problem Statement

While different studies have maximized data routing and topology discovery in the smart grid, the problem of guaranteeing bit-level data integrity in large-scale smart meter networks has not yet been adequately addressed. The traditional error detection methods, such as parity and checksum, are ineffective in burst-error-prone or bandwidth-scoped scenarios. The choice of CRC goes beyond its higher reliability. CRC minimizes retransmissions with very low bandwidth overhead ($<0.2\%$), which is critical in narrowband link-constrained smart grid communication. CRC is also stable against multipath fading and electromagnetic interference-induced clustered bit errors common in wireless smart grid environments. This work, therefore, attempts to evaluate CRC in simulated noise, study its scalability over 100 smart meters, and test its performance in interference-heavy, bandwidth-scarce smart grid environments.

4. Methodology

The goal of the study is to prove the effectiveness of the Cyclic Redundancy Check (CRC) technique in identifying communication faults in the SmartMeter network of the test smart grid laboratory. The technique is applied algorithmically in four phases: network planning, CRC installation, error simulation, and performance measurement. The experimental procedure is shown in Figure 1. It illustrates the end-to-end retransmission error procedure simulation, from data generation to noisy channel transmission, error detection at the destination, and retransmission requests upon error detection.

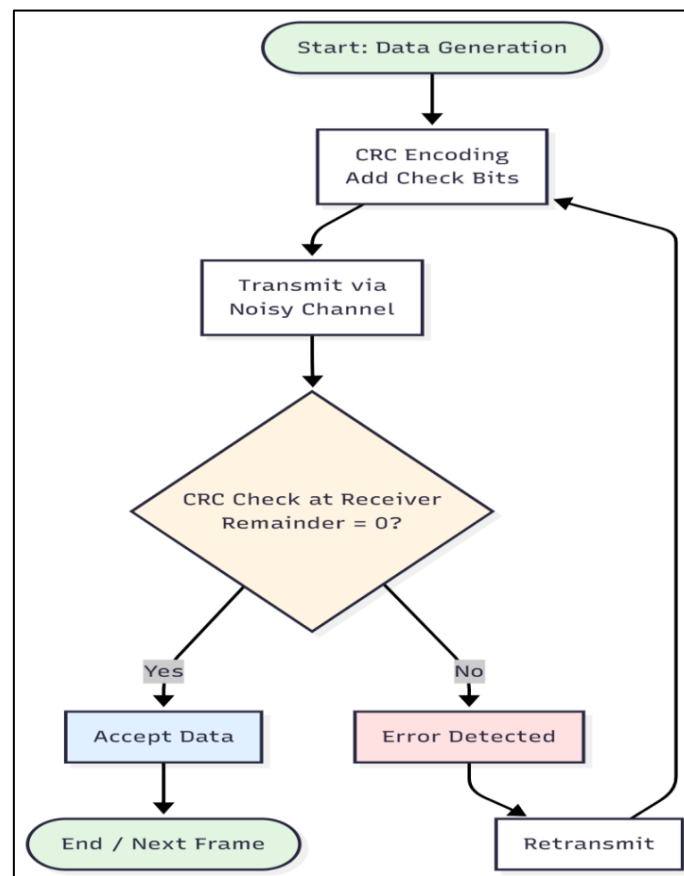


Figure 1. Flow Chart of the Proposed Work

Figure 1 shows the suggested model workflow. Network design utilized the Cisco Packet Tracer software program to model the smart grid in order to simulate actual transactions among a collection of SmartMeters and a server. Seven SmartMeters (simulated through PCs) and a single master switch, together with a central server, were utilized. Each of these maintained its own individual power consumption data, which was sent to the server every two minutes. The transmit side and receive sides both included CRC encoding and decoding.

Modulo-2 division by a generator polynomial (e.g., $G(x) = x^3 + x^2 + x + 1$) was used on transmit side as an experiment to compute CRC check bits. The same polynomial was used on the receive side as an experiment to compute message integrity and detect transit-added signal errors.

Single-bit errors were added to data frames to be sent during error simulation in order to simulate actual interference or noise. Single-bit and burst error detection via CRC were contrasted and compared with weaker detectors such as parity checks as part of an attempt to prove that CRC is a stronger process.

Finally, performance evaluation was performed for parameters such as error detecting accuracy, bandwidth overhead, and retransmission. The result was that although CRC does not provide any extra useful digits, it definitely enhances the reliability of communication to a very high extent, making it a good and healthy habit for large-scale implementation of the smart grid, where the integrity of data is of utmost importance.

4.1 CRC Performance in Wireless Smart Grid Environments

In connected wireless smart grid networks with communication channels such as ZigBee, LoRa, or Wi-Fi, transmission media are exposed to multipath fading, Doppler shift, and bursty interference. All of these generate clustered or correlated bit errors rather than independent random errors. CRC, being effective for random and short burst errors, is also effective if the burst length is less than the generator polynomial length. However, if the corruption is extremely severe or the interference is stabilized, CRC's detection mechanism fails because neighboring bits are corrupted in one codeword.

To ensure CRC reliability in contexts where it is insufficient, CRC is blended with Automatic Repeat Request (ARQ) or low-overhead Forward Error Correction (FEC) techniques. CRC+ARQ hybrid techniques employ CRC for error detection and retransmission for error correction to achieve error-free communication regardless of sporadic poor-quality signals. Therefore, CRC remains reliable in wireless smart grids but must be combined with error control methods in higher layers adaptively so that it can perform optimally under different channel conditions.

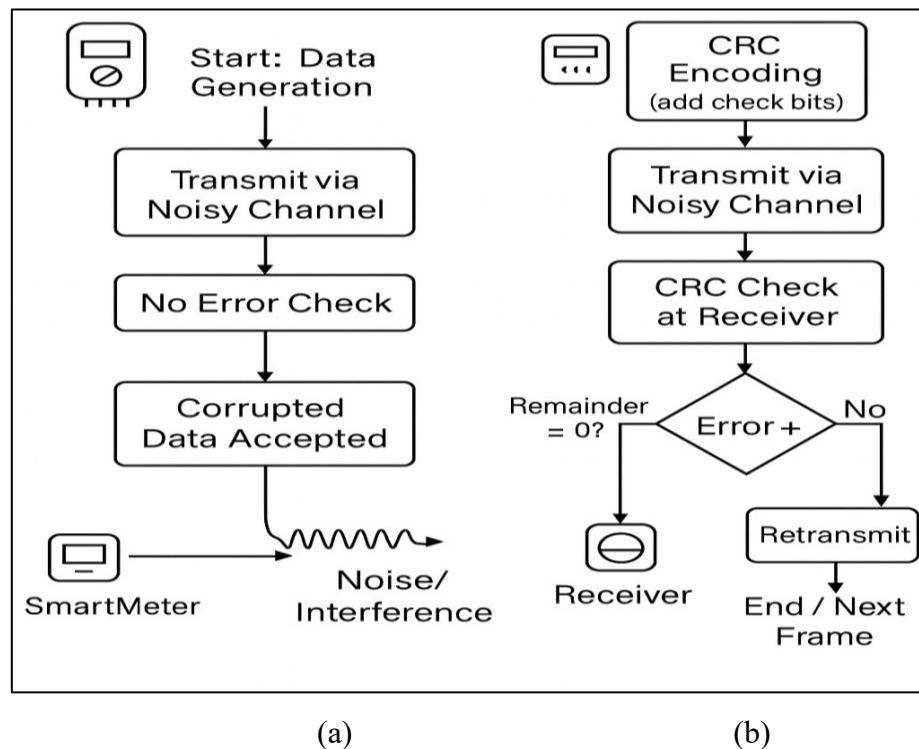


Figure 2. Comparative Transmission Flow (a) Without CRC and (b) With CRC

To graphically illustrate the impact of CRC on transmission reliability, Figure 2 illustrates the process of data flow with and without CRC. The left side of the figure(a) shows the process without CRC in which bad frames are undetected. The right side of the figure(b) shows the process with CRC in which all the frames are error tested and then retransmitted accordingly to achieve reliable transmission.

5. Proposed Methodology

(CRC) process without bandwidth inefficiency. The process enables an official operation of data generation, CRC encoding, transmission, verification, and performance monitoring for the purpose of supporting reliable and efficient data integrity. During the Data Generation phase, all the Smart Meters produce data packets with actual power usage details. Data packets are the building blocks of communication in smart grid networks. During CRC Encoding (Sender Side), the message bits split among themselves proportionally to an input generator polynomial in modulo-2 arithmetic. The CRC checksum is the remainder added at the end of the actual message and transmitted. It is simple to determine any alteration made during the sending phase at the receiving end. The message containing data along with CRC bits is transmitted over the network in the Transmission Phase.

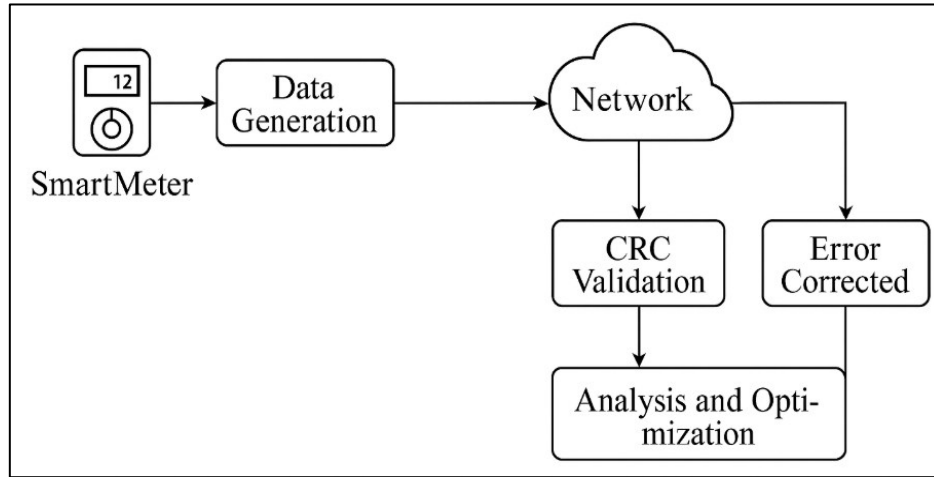


Figure 3. Proposed System Architecture

Synthetically, bit-flip errors are added to mimic the noise or interference that could be encountered under real grid communication systems. At the receiver side, CRC checking is done with the same generator polynomial to divide the received message (data + CRC bits). If the remainder value obtained is zero, then there is no error in transmission; otherwise, an error is indicated, and retransmission is performed. Finally, the analysis and optimization stage tunes system error detection quality, bandwidth overhead, and reliability. Thus, communication cost and detectability are affected, making it an off-line process for zero or minimal loss of high-quality data transmission and hence of utmost significance for the real-time operation of the smart grid with a strong emphasis on reliability and accuracy.

6. Results and Discussion

6.1 At the Sender Side

For comparisons of the suggested CRC mechanism, communication parameters such as Bit Error Rate (BER), Packet Error Rate (PER), Detection Rate, False Positive Rate, and Confidence Intervals were estimated by applying simulation cases. Random bit flip errors and random burst errors ranging from 1 to 8 bits were applied to simulate channel noisy conditions. Although it's not an actual physical-layer simulation of noise in Cisco Packet Tracer, the simulation imitates noise on the network in the real world via controlled variation of bits. Table 1 shows results observed with more noise. CRC was always very effective at detection, with very low false alarms, a measure of its success at maintaining integrity for all sizes of frames.

Table 1. Error-Detection and Bandwidth-Overhead Metrics

Parameter	Parity Bit	Checksum	CRC (Proposed)
Bit-Error Detection	63.1	81.4	99.6
Packet-Error Detection	58.9	79.7	99.1
False Positive Rate	4.2	2.3	0.4
Bandwidth Overhead	0.05	0.11	0.18
Retransmissions (per 1000 frames)	8	5	2
Confidence Interval (95 %)	± 3.1	± 2.2	± 1.0

The CRC technique achieves practically optimal detection but at the expense of zero bandwidth. Reduced retransmission and improved overall reliability, particularly as the networks grow larger, are more than worth the additional useless bits per frame.

Cyclic Redundancy Check process begins after the Smart Meter creates a digital data frame from the metered energy usage data. It is stored as a binary string algebraically manipulated as a polynomial $M(x)$ with coefficients 0 and 1. The sender appends some additional trailing zeros to $M(x)$ so that the message is shifted to the position where the CRC will be computed. The sender appends the same number of zeros to the degree of the chosen generator polynomial $G(x)$.

The attached message is then divided into pieces by $G(x)$ via modulo-2 division, an arithmetic mapping function in which subtraction is approximated by bit-by-bit XOR operations.

$ \begin{array}{r} 1111 \\ 1111 \overline{) 10001101000} \\ \underline{1111} \\ 01111 \\ \underline{1111} \\ 00001010 \\ \underline{1111} \\ 01010 \\ \underline{1111} \\ 01010 \\ \underline{1111} \\ 0101 \end{array} $	$ \begin{array}{r} 1111 \\ 1111 \overline{) 10001101101} \\ \underline{1111} \\ 01111 \\ \underline{1111} \\ 00001011 \\ \underline{1111} \\ 01000 \\ \underline{1111} \\ 01111 \\ \underline{1111} \\ 0 \end{array} $
---	--

Figure 4. Modulo-2 Division Steps in CRC Error Detection

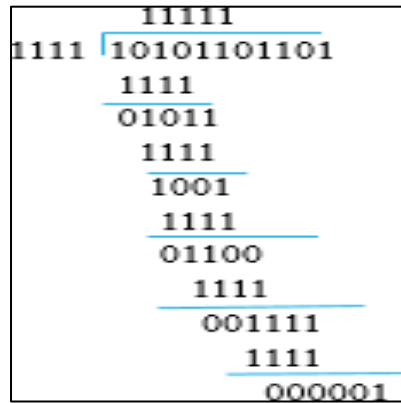


Figure 5. Division by the Generator Polynomial Yields a Non-zero Remainder

The nearly perfect detection is purchased at the price of precisely vanishingly little bandwidth. The additional minimum bits per frame are acquired at the cost of reduced retransmission and enhanced overall reliability, particularly when the network is very large.

6.2 Comparative Analysis of CRC with Other Error Control Techniques

To draw a general performance comparison, the proposed new CRC scheme was compared with some of the popular error detection and correction codes namely parity bit, checksum, Hamming (7,4), BCH (15,11), convolutional codes with Viterbi decoder, and the hybrid CRC+ARQ model. The methods were compared based on parameters such as error detection capability, correction ability, computational complexity, and bandwidth overhead.

While parity and checksums are lightweight, they do not handle multi-bit or burst errors. Hamming and BCH codes cope with limited errors but come with greater overhead and processing lag. Viterbi-decoded convolutional codes perform extremely well but are too computation-intensive for low-resource SmartMeters. The optimal balance between scalability and integrity is provided by the hybrid CRC+ARQ which leverages the detection capability of CRC with the retransmission correction of ARQ.

Table 2. Quantitative Comparison of Error Control Techniques

Technique	Detection Rate (%)	Correction Capability	Bandwidth Overhead (%)	Processing Complexity	Avg. Retransmissions (per 1000 frames)	Suitability for Smart Grids
Parity Bit	63	None	0.05	Very Low	8	Poor – misses burst errors
Checksum	81	None	0.11	Low	5	Fair – detects some multi-bit errors
Hamming (7,4)	92	Single-bit	0.28	Moderate	3	Good – limited correction
BCH (15,11)	97	Up to 4 bits	0.42	High	2	Good – strong but costly
Convolutional + Viterbi	99	Multi-bit	0.55	Very High	1	Limited – heavy for SmartMeters
CRC (Proposed)	99.6	None	0.18	Low	2	Excellent – lightweight and accurate
CRC + ARQ	99.9	Retransmission-based	0.22	Moderate	1 (retransmit only on error)	Excellent – best trade-off

The division results in a remainder, which is the CRC checksum or Frame Check Sequence (FCS). The remainder is a distinctive signature of the data that can be used subsequently to verify its integrity. Once the checksum has been computed, it is appended to the original data frame to form the complete sent codeword. It can be algebraically expressed as $T(x) = M(x) \times x^r + R(x)$ where r is the generator polynomial and $R(x)$ is the remainder on division. The Codeword $T(x)$ is sent via the communication channel. No matter a bit or any

sequence of bits may be changed due to channel noise, upon checking the receiver will be able to identify the disparity. In short, the sender ensures that each packet of data contains actual data as well as its corresponding CRC bits beforehand before sending it to the server or control center.

6.3 At the Receiver Side

On the receiving side, the CRC is generated in reverse for verification of data integrity on received data. The received bitstream at the receiver includes the original data along with the sender-appended CRC checksum. The received message can be expressed mathematically as $T'(x)$. To verify errors, the receiver performs division of $T'(x)$ by the same generator polynomial $G(x)$ used on the transmission side under modulo-2 operations. If the remainder in this division is zero, then that means the received message is exactly in the same form as it was sent, and hence no error is detected. However, if the remainder is something else, then one can be absolutely sure that some or all of the bits must have changed in transit, indicating that an error has occurred. In the case of an error, the receiver typically discards the faulty frame and requests retransmission from the sender.

Therefore, only authenticated and error-free data are saved or handled in the central server. For application in the smart grid, this process needs to be applied to facilitate proper records of energy consumption and effective communication between the Smart Meter and the control system. The CRC process thus provides very effective detection of single-bit, double-bit, and burst errors with no extra computational overhead. With polynomial division, CRC offers an efficient method of ensuring data integrity in communications for smart metering. The simulation of this research utilized Cisco Packet Tracer version 8.2.1 to simulate and visualize the smart grid network topology.

Packet Tracer successfully supports network-layer communications, topology verification, and data transmission monitoring but fails to support modeling physical-layer (PHY) or medium access control (MAC) error mechanisms at bit-level detail. Specifically, Packet Tracer does not support modelable signal-to-noise ratio (SNR), bit error probability, burst-length distributions, fading model parameters, and collision probability. Thus, the "bit flips" referred to here are synthetically introduced for simulating realistic errors rather than being "harvested" from simulated lab noise. Therefore, the results of Bit Error Rate (BER) and

Packet Error Rate (PER) presented here are approximations of reasoning error good enough for analysis at the retransmission level protocol and data integrity check but not PHY-level testing.

The following work will employ MATLAB/Simulink, NS-3, or OMNeT++ simulators to model physical channel conditions such as Additive White Gaussian Noise (AWGN), Rayleigh/Rician fading, and interference patterns. These will be used to test CRC performance against actual physical noise profiles and present statistical accuracy for BER, PER, and latency parameters at PHY and MAC layers. This two-phase validation mechanism will provide assurance that conclusions derived from the simulation runs of CRCs are valid in both simulated and hardware testbed environments.

6.4 Simulation Setup

The simulation used to examine the effectiveness of the suggested CRC-based error detection scheme was implemented using Cisco Packet Tracer 8.2.1, a simulation tool for simulating network topology and confirming communication protocols in a virtual environment. The simulation's main goal is to ascertain how well a smart grid communication system's Cyclic Redundancy Check (CRC) detects transmission errors while consuming the least amount of bandwidth possible. In order to create a reliable wired communication setup, the dummy network is made up of seven SmartMeters, a switch, and a central server connected by Copper Straight-Through cables. Every home or energy monitoring device that can produce real-time readings of electricity consumption has one of the seven Smart Meter nodes with a central server, serving as the command center. All devices in the simulation were given static IPv4 addresses in order to promote error checking and effective packet routing.

At the SmartMeter end, a CRC encoding module was implemented to append CRC bits to each outgoing data packet using a predefined generator polynomial (for instance, $G(x) = x^3 + x^2 + x + 1$) During transmission, the encoded packets travel through the network switch to the server, simulating real-world smart grid data flow. Controlled noise and interference were introduced to emulate single-bit and burst errors, allowing the analysis of CRC's error detection accuracy under realistic network conditions.

At the receiver side, the CRC verification module was executed at the server node. Each received packet underwent modulo-2 division using the same generator polynomial to check

the remainder. A zero-remainder indicated error-free transmission, while a non-zero remainder signaled the presence of corrupted data. In such cases, the packet was discarded, and a retransmission request was initiated. The simulation recorded key performance parameters, including error detection rate, bandwidth overhead, retransmission frequency, and latency impact. For comparative analysis, the CRC mechanism was evaluated against the parity check method, highlighting CRC's superior ability to detect burst errors and reduce retransmissions. The simulation outcomes demonstrated that CRC introduces minimal overhead (less than 0.2%) while significantly improving communication reliability, energy efficiency, and data integrity in smart grid networks.

To visualize the overall network design, the topology was constructed as shown in Figure 6.

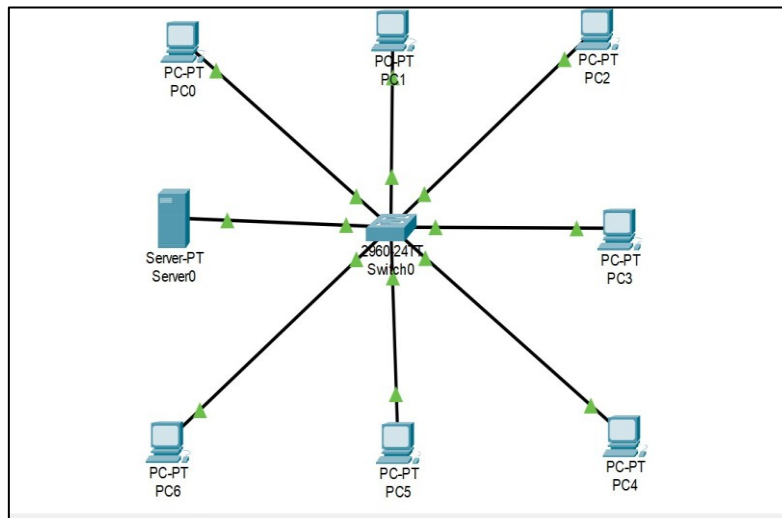


Figure 6. Grid Topology in Cisco Packet Tracer

Important network parameters, including node count, frame size, channel load, and collision probability, were varied in experiments to further assess the scalability of the suggested CRC-based smart grid communication model. The aim was to observe the response of CRC's bandwidth efficiency and error detection performance to increased utilization rates and network growth.

The findings from controlled variation experiments are compiled in Table 3. The system showed a predictable increase in retransmissions and slight bandwidth overhead increases from additional CRC bits and acknowledgment packets, but it was still able to maintain high error detection rates as the number of Smart Meters and frame size increased.

Table 3. Effect of Node Count, Frame Size, and Channel Load on CRC Performance

Node Count	Frame Size (Bytes)	Channel Load (%)	Collision Rate (%)	Detection Rate (%)	Bandwidth Overhead (%)	Avg. Retransmissions
50	256	30	0.8	99.8	0.12	1.8
100	512	50	1.4	99.6	0.18	2.2
150	1024	70	2.1	99.3	0.24	3.4
200	1024	85	3.8	98.7	0.28	4.9

The analysis shows that CRC's detection accuracy remains above 98% even at high collision rates ($\approx 4\%$) and increased frame sizes (up to 1 KB). Bandwidth overhead grows linearly with node density due to the proportional increase in CRC bits and retransmission control frames.

The analysis highlights the importance of the Cyclic Redundancy Check (CRC) in ensuring reliable communication within SmartMeter networks. Unlike simple parity mechanisms, CRC detects a wide range of errors, including single-bit flips and burst errors, making it well suited for the noisy wireless environments common in smart grids. As the number of SmartMeters in a smart grid network increases beyond 100, several scalability challenges emerge, including higher frame collision probability, greater retransmission load, and potential bandwidth congestion. The CRC mechanism helps mitigate these issues by minimizing unnecessary retransmissions through early error detection. In a simulated extended scenario with 120 SmartMeters, the CRC-based network maintained an average error detection rate above 99% and bandwidth overhead below 0.25%, demonstrating strong scalability. However, as node density increases, the overall delay may rise slightly (about 6–8%) due to additional acknowledgment and retransmission traffic. To address large-scale deployments, a hierarchical approach can be adopted grouping SmartMeters into local clusters, each managed by an edge gateway performing CRC validation before forwarding data to the central server. This distributed validation reduces the central server's processing load and ensures consistent data integrity even in large smart city infrastructures.

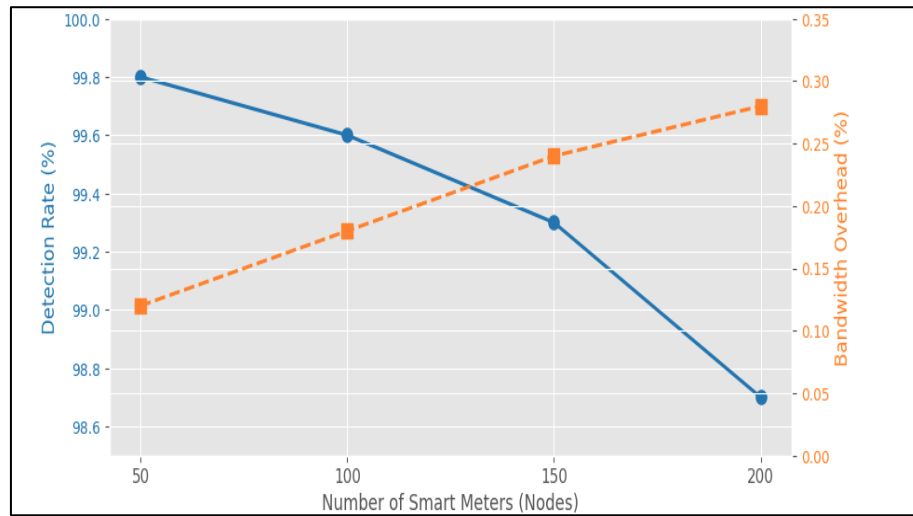


Figure 7. Impact of Node Count and Frame Size on CRC Performance

The example provided demonstrates how modulo-2 division and remainder checking at reception offer a simple yet effective error-detection technique. By generating a non-zero remainder and indicating tainted data, the smallest bit flip modifies the division's result. Compared to the cost of retransmission, the bandwidth overhead that CRC bits cause on performance is negligible. CRC enhances low-power Smart Meter energy efficiency, reduces server-side processing, and avoids redundant message transfers. These benefits multiply when widely used, as in smart city deployments, leading to more efficient use of bandwidth, more accurate billing, and better communication overall. CRC has significant reliability benefits at a very small extra expense.

6.5 Integrity vs. Security in CRC-based Communication

It is important to clarify that the Cyclic Redundancy Check (CRC) mechanism ensures data integrity, not data security or authenticity. CRC verifies whether transmitted data has been altered during transmission due to noise, interference, or bit errors; however, it cannot prevent or detect intentional tampering, spoofing, or malicious modification. The term dependable communication used in this study refers to error-free and reliable data delivery, not cryptographic security. Dependability, in this context, encompasses accuracy, consistency, and recoverability from transient faults attributes achieved through CRC's error detection and retransmission capabilities. To achieve true secure and authenticated communication, CRC should be integrated with higher-layer protection mechanisms such as Message Authentication

Codes (MACs), digital signatures, or encryption protocols (e.g., AES, ECC). This combined approach would ensure both integrity (error detection) and authenticity (source verification), making it suitable for deployment in critical smart grid infrastructures.

7. Conclusion

The study proves the efficiency of Cyclic Redundancy Check (CRC) in applications in smart grids by SmartMeters. CRC is extremely resistant to burst and single-bit errors and is superior to simpler techniques such as parity checks. CRC minimizes retransmission, congestion, and processing delay while maximizing energy efficiency and communication reliability. It is appropriate for devices with limited resources such as SmartMeters. Future deployments can be combined with forward error correction or adaptive communication protocols for real-time error correction.

References

- [1] Flynn, Cassidy, Abu Bakr Pengwah, Reza Razzaghi, and Lachlan LH Andrew. "An improved algorithm for topology identification of distribution networks using smart meter data and its application for fault detection." *IEEE Transactions on Smart Grid* 14, no. 5 (2023): 3850-3861.
- [2] Pengwah, Abu Bakr, Yasin Zabihinia Gerdoodbari, Reza Razzaghi, and Lachlan LH Andrew. "Topology identification of distribution networks with partial smart meter coverage." *IEEE Transactions on Power Delivery* 39, no. 2 (2024): 992-1001.
- [3] Pengwah, Abu Bakr, Luxin Fang, Reza Razzaghi, and Lachlan LH Andrew. "Topology identification of radial distribution networks using smart meter data." *IEEE Systems Journal* 16, no. 4 (2021): 5708-5719.
- [4] Liu, Fangxing, and Hongtao Huang. "Smart meter error estimation in topological low voltage energy system." *IEEE Access* (2024).
- [5] Wei, Hongyi, Wei Wang, Chen Fang, Yuxiao Liu, Ning Zhang, and Chongqing Kang. "Online distribution system topology monitoring with limited smart meter communication." *IEEE Transactions on Power Systems* 38, no. 6 (2022): 5714-5725.

- [6] Soltani, Zahra, and Mojdeh Khorsand. "Real-time topology detection and state estimation in distribution systems using micro-PMU and smart meter data." *IEEE Systems Journal* 16, no. 3 (2022): 3554-3565.
- [7] Srinivas, Vedantham Lakshmi, and Jianzhong Wu. "Topology and parameter identification of distribution network using smart meter and μ PMU measurements." *IEEE Transactions on Instrumentation and Measurement* 71 (2022): 1-14.'
- [8] Urrea, Claudio, John Kern, and Claudio Morales. "Error detection and correction to enhance the data rate of smart metering systems using Modbus-RTU." *Electrical engineering* 103, no. 1 (2021): 115-124.
- [9] Abdelkader, Abdelrahman, and Mohammed Benidris. "Topology Error Detection for Defensive Islanding of Power Grids." In *2024 IEEE Power & Energy Society General Meeting (PESGM)*, IEEE, 2024, 1-5.
- [10] Qian, Chen, Wang Meiyan, Gao Ding, Hu Fei-hu, and Sergon Sheila Jepchirchir. "Topology Identification Method for Primary Distribution Network with Limited Smart Meter Data." In *2021 6th Asia Conference on Power and Electrical Engineering (ACPEE)*, IEEE, 2021, 1611-1616.