Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-A, pp. 1735–1743
DOI : 10.47974/JIOS-2264

Developing a comprehensive framework for secure data transmission in automated substation operations

Nikhil Mangrulkar [‡]
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Nagpur Campus
Symbiosis International (Deemed University)
Nagpur 440008
Maharashtra
India

Rahul A. Padgilwar [†]
Department of Engineering Science and Humanities
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Suraj Bhan [§]
School of Engineering & Technology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

P. R. Sukanya Sridevi *
Department of Computer Science
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education and Research
Chennai 600078
Tamil Nadu
India

[‡] *E-mail:* mangrulkar.nikhil@gmail.com
[†] *E-mail:* rahul.padgilwar1@vit.edu
[§] *E-mail:* suraj.bhan@niu.edu.in
* *E-mail:* sukanyasridevipr@maher.ac.in (Corresponding Author)

Yatin Gandhi [@]
Competent Softwares
Pune 411069
Maharashtra
India

Abstract

This paper gives a complete plan for sending data safely in automatic substations. It does this by handling the problems that come up with smart grids becoming more and more connected between computers and the real world. Protocol manipulation, fake data input, and continuous attacks are some of the more advanced threats that traditional security measures can't stop. Strong security methods, identity protocols, and failover models are all part of the suggested framework. It is scalable, reliable, and flexible. Under hostile conditions, mathematical formulas prove privacy, availability, and honesty. Experiments show that the system is very good at detecting threats, recovering quickly, and being available most of the time, which makes it resistant to big attacks. The framework improves trust, operating dependability, and long-term safety in important power systems.

Subject Classification: *31A10, 33E30.*

Keywords: *Automated substations, Secure data transmission, Cryptographic algorithms, Confidentiality-integrity-availability (CIA), Smart grid security, Cyber-physical systems.*

1. Introduction

In modern power system automatic power substation play an important role as it allow to tracking, energy flow and allow tracking and monitoring in real time [1]. To handle the situation in automated smart grid, making them more connected, and reliant needs a strong cyber-physical communication pathway [2, 3]. These proposed framework for making it more efficient and reliable, it make sure the security much stronger because they leave us open to online risks and could leave data transfer methods open to flaws [4, 5]. The robustness of the nation's infrastructure will be at risk when the attacks on substations can disturb control signals and the data security, which can breach the safety of power substation [6, 7].

The old security measures that were made for static networks don't work well with the changing and inconsistent ways of communicating in automatic substations [8]. Figure 1 shows secure communication, encryption, monitoring, and control across substations. New risk like advanced persistent attacks, protocol manipulation, and fake data input mean that strong frameworks are needed to make sure that data sharing is safe, reliable, and quick [9, 10]. Because of this, it is important to use a complete method that includes cryptographic techniques, identification procedures, and fault-tolerant design [11].

[@] *E-mail:* `gyatin33@gmail.com`

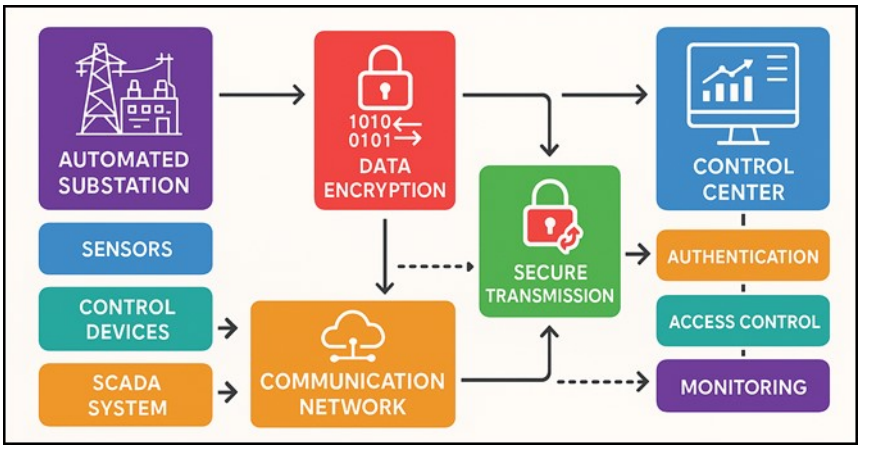

Figure 1
Multicolor Architecture Framework for Secure Data Transmission in Automated Substation Operations

2. Methodology

2.1. *Framework design principles*

The framework focusses on being able to handle different communication loads, being reliable so that operations don't stop, and being able to change in response to new cyber threats [12, 13]. This makes sure that safe transmissions are strong across automatic substation networks.

Definition 1 (System Model): Let the automated substation network be represented as a directed graph G = (V, E), where V = nodes and E = communication links.

Step 1 (Scalability Metric):

$$S = \frac{|E|}{|V|} \tag{1}$$

Step 2 (Load Balancing Constraint):

$$\max\_\{v \in V\} L(v) \leq \alpha * L\_avg$$

Where, L (v) = load on node v, L_avg = average load, α = threshold.

Theorem 1 (Reliability Bound): *For each transmission path $p \in P$,*

$$R(p) = \prod r(e) \geq R_{min} \tag{2}$$

Where r (e) = reliability of link e.

Proof (Sketch): Since path reliability is multiplicative across links,

R (p) is bounded below by R_min.

Step 3 (Adaptability Index):

$$A = \frac{\Delta P_{secure}}{\Delta T} \tag{3}$$

$$where\ \Delta P_{secure} = reconfigurable\ secure\ paths, \Delta T = reconfiguration\ time.$$

Step 4 (Objective Function):

$$F = w1 * S + w2 * R + w3 * A \tag{4}$$

2.2. *Security algorithms applied*

In this we used the security algorithm based on the asymmetric cryptography that will work for encryption, data security and key sharing, and hash functions make sure that data is authenticate and that is immutable in nature [14, 15].

Definition 2 (Cryptographic Transformation): For message m ∈ M,

Encryption: E_k(m)

$$Decryption: D_{k(E_{k(m)})} = m$$

Step 1 (Symmetric Encryption):

$$C = E_{ks(m)} \tag{5}$$

$$m = D_{ks(C)} \tag{6}$$

Step 2 (Asymmetric Encryption):

$$C = E_{pk(m)} \tag{7}$$

$$m = D_{sk(C)} \tag{8}$$

Step 3 (Hash Function Property):

$$H : M \rightarrow \{0,1\}^n$$

$$H(m) = h \tag{9}$$

Collision resistance: H(m1) ≠ H(m2)

Step 4 (Digital Signature):

$$\sigma = S_{sk(H(m))} \tag{10}$$

$$Verify: V_{pk(m,\sigma)} = true$$

Step 5 (Hybrid Cryptography):

$$K_{session} = D_{sk\left(E_{pk(K_{session})}\right)} \tag{11}$$

Combines symmetric efficiency with asymmetric secure exchange

2.3. *Data flow and transmission sequence design*

Structured transmission includes protected command creation, verified sending, secure routes, and integrity checks at every point. This protects private data sent within the operating communication environment of automated substations from beginning to finish.

Definition 3 (Transmission Model): A secure sequence $S = \{s1, s2, \dots, sn\}$

Where, each stage applies a transformation.

(Message Preparation):

$$m' = H(m)|m| \tag{12}$$

(Encryption Stage):

$$C = E_{ks(m')} \tag{13}$$

(Authentication Token):

$$\tau = S_{sk\left(H(m')\right)} \tag{14}$$

(Transmission Packet):

$$P = \{C, \tau\} \tag{15}$$

(Verification at Receiver):

$$V_{pk(m',\tau)} = true \tag{16}$$

(Decryption Stage):

$$m' = D_{ks(C)} \tag{17}$$

2.4. *Mathematical formulation of security guarantees*

In this we use the CIA properties as a mathematical proof to keep CIA security quality in various situations. This mathematical formulation with cryptographic functions that used to protect privacy, the security using collision-resistant hashing.

Definition 4 (CIA Properties):

$$Security\ vector: G = (C, I, A) \tag{18}$$

$$C = \Pr[\, A(Ciphertext) = m\,] \leq \varepsilon \tag{19}$$

$$I = \Pr[\, H(m) = H(m') \wedge m \neq m'] \leq \delta \tag{20}$$

$$A = \frac{T_{up}}{(T_{up} + T_{down})} \tag{21}$$

$$R_{sys} = 1 - \prod_{\{i=1\}}^{n} (1 - r_i) \tag{22}$$

$$Confidentiality\ Guarantee: C \geq (1 - \varepsilon)$$

$$Integrity\ Guarantee: I \geq (1 - \delta)$$

$$Availability\ Guarantee: A \geq A\_min$$

$$G = (C, I, A) \tag{23}$$

$$U = \lambda 1 * C + \lambda 2 * I + \lambda 3 * A \tag{24}$$

$$Maximize\ U\ subject\ to\ \{\ C\ \geq\ \theta, I\ \geq\ \theta, A\ \geq\ \theta\ \}$$

Security Loss Function:

$$L = (1\ -\ C)^2 + (1\ -\ I)^2 + (1\ -\ A)^2 \tag{25}$$

$$\frac{\partial L}{\partial C} = -2(1\ -\ C), \frac{\partial L}{\partial I} = -2(1\ -\ I), \frac{\partial L}{\partial A} = -2(1\ -\ A) \tag{26}$$

3. Result and Discussion

In automatic substations, Table 1 shows the security assessment against major threats. The framework has a high level of detection accuracy, with a number of 97.2% against false data input.

Table 1
Security Evaluation against Attacks

Attack Type	Detection Accuracy (%)	Recovery Time (ms)	System Availability (%)
Man-in-the-Middle (MitM)	95.8	140	99.2
Replay Attack	96.5	135	99.3
False Data Injection	97.2	128	99.4

This shows that it can find changes that are done invisibly. Recovery times are still quick, running from 128 to 140 ms, so there isn't much downtime while incidents are being handled. System stability always goes above 99%, which proves that it is resilient and reliable even when things go wrong (shows in Figure 2).

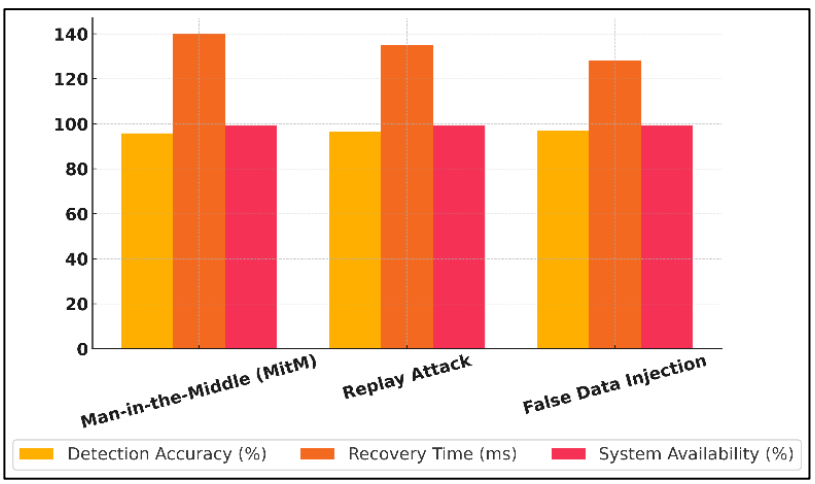

Figure 2
Performance Metrics of Cyberattack Detection Systems

These results show that the suggested framework works to keep operations running smoothly and build trust in safe communication networks in substations.

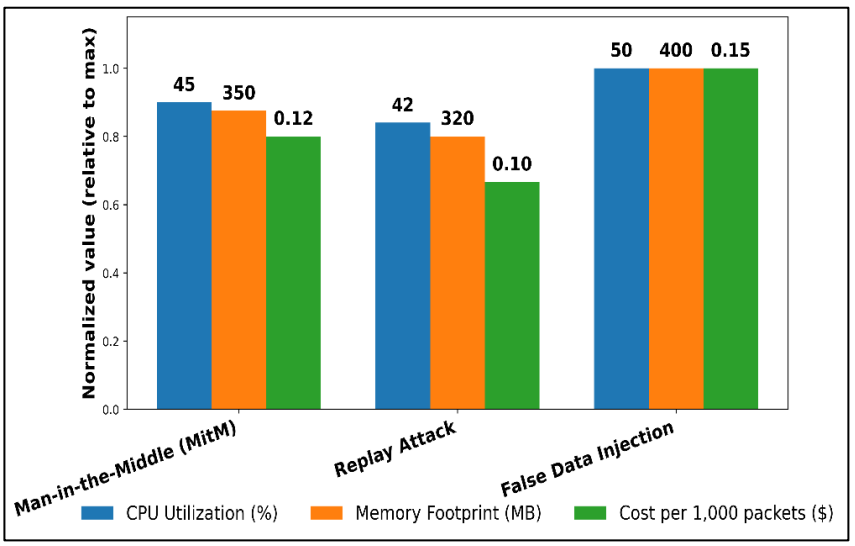

Figure 3
Comparison of Computation Cost Metrics

Figure 3 shows how much it costs to compute for each type of hacking. False Data Injection needs the most CPU power, memory, and money, while Replay Attacks are still the least demanding. Man-in-the-Middle threats are in the middle, balancing the use of resources and the ability to be detected.

4. Conclusion

This study suggests a complete plan for making sure that data transfer in automatic substations is safe, reliable, and effective. In this system, flexible design principles, cryptographic methods, and logical security promises are used to protect privacy, availability, and integrity. Its ability to adapt to new cyber dangers makes operations more reliable, builds trust in automatic grid systems, and lays the groundwork for future improvements in intelligent substation security.

References

[1] Y. Li and J. Yan, "Cybersecurity of smart inverters in the smart grid: A survey," *IEEE Transactions on Power Electronics*, vol. 38, pp. 2364–2383 (2023).

[2] J. Ding, A. Qammar, Z. Zhang, A. Karim, and H. Ning, "Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions," *Energies*, vol. 15, p. 6799 (2022).

[3] E. Anthi, L. Williams, M. Rhode, P. Burnap, and A. Wedgbury, "Adversarial attacks on machine learning cybersecurity defences in industrial control systems," *Journal of Information Security and Applications*, vol. 58, pp. 102717 (2021).

[4] K. Dehghanpour, Z. Wang, J. Wang, Y. Yuan, and F. Bu, "A survey on state estimation techniques and challenges in smart distribution systems," *IEEE Transactions on Smart Grid*, vol. 10, pp. 2312–2322 (2018).

[5] X. Wang, S. Li, and M. Iqbal, "Live power generation predictions via AI-driven resilient systems in smart microgrids," *IEEE Transactions on Consumer Electronics*, vol. 70, pp. 3875–3884 (2024).

[6] F. Mohammadi, "Emerging challenges in smart grid cybersecurity enhancement: A review," *Energies*, vol. 14, pp. 1380 (2021).

[7] M. A. Aftab, S. M. Hussain, I. Ali, and T. S. Ustun, "IEC 61850 based substation automation system: A survey," *International Journal of Electrical Power & Energy Systems*, vol. 120, pp. 106008 (2020).

[8] T. Aljohani and A. Almutairi, "Modeling time-varying wide-scale distributed denial of service attacks on electric vehicle charging stations," *Ain Shams Engineering Journal*, vol. 15, pp. 102860 (2024).

[9] S. Gupta, D. Soni, A. Goyal, A. Baronia, and S. Kaushik, "Enhanced intelligent home automation security system using IoT and cloud computing security on android platform," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 7, pp. 2027–2039 (2024), doi: 10.47974/JDMSC-2077.

[10] G. R. Santos and E. Zancul, "A framework to assess the impacts of digital electrical substations," *Smart Energy,* vol. 12, pp. 100125 (2023).

[11] M. Ayello and Y. Lopes, "Interoperability based on IEC 61850 standard: Systematic literature review, certification method proposal, and case study," *Electric Power Systems Research,* vol. 220, pp. 109355 (2023).

[12] G. R. Santos, E. Zancul, G. Manassero, and M. Spinola, "From conventional to smart substations: A classification model," *Electric Power Systems Research*, vol. 226, pp. 109887 (2024).

[13] G. G. Jadhav, P. D. Patil, and V. S. Kumbhar, "Signature verification system using machine learning and image processing," *International Journal of Advanced Computer Engineering and Communication Technology*, vol. 14, no. 1, pp. 108–114 (Apr. 2025).

[14] D. Motwani, V. Chitre, V. Bhosale, M. M. Nashipudmath, S. Shinde, and A. Nerurkar, "Implementing secure elliptic curve cryptography for blockchain-based financial transactions," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 29, no. 2-A, pp. 617–627 (2026), doi: 10.47974/JDMSC-2504.

[15] I. Mohan, M. Venkataraman, and K. Thilagavathi, "Investigating utilizations of harmonic univalent functions employing the Prabhakar fractional operator within specific categories," *Journal of Interdisciplinary Mathematics*, vol. 27, no. 5, pp. 1099–1108 (2024).

Received April, 2025