Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3027–3036
DOI : 10.47974/JDMSC-2639

Trust-aware ad hoc network security using random bit operations and RC4 stream cipher framework

Prashant Vats [#]
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Naveen Tewari [†]
Department of Computer Applications
School of Computing
Graphic Era Hill University
Bhimtal Campus
Nagri Gaon 263132
Uttarakhand
India

Surabhi Shanker [§]
Centre of Excellence - Cyber Security
School of Engineering & Technology
K. R. Mangalam University
Gurugram 122103
Haryana
India

Devesh Kumar Srivastava [‡]
Department of Information Technology
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

[#] *E-mail:* prashant.vats@jaipur.manipal.edu
[†] *E-mail:* navtewari@gmail.com
[§] *E-mail:* surabhi.shanker@krmamgalam.edu.in
[‡] *E-mail:* devesh.srivastava@jaipur.manipal.edu

Madan Lal Saini [@]
Department of Computer Science and Engineering
Apex Institute of Technology (AIT)
Chandigarh University
Mohali 140413
Punjab
India

Ashok Kumar Saini*
Department of Computer Science and Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Abstract

In dynamic and decentralized environments such as ad hoc networks, ensuring secure communication and mutual trust among nodes presents a significant challenge due to the absence of centralized control and frequent topology changes. This paper proposes a Trust-Aware Security Framework that integrates Random Bit Operations with the RC4 Stream Cipher to enhance confidentiality, authenticity, and trustworthiness in node-to-node communication. The proposed model employs random bit manipulation during the key generation and encryption phases to increase entropy and resist statistical and correlation attacks typically associated with traditional RC4 implementations.

Subject Classification: *Primary 94A60, Secondary 68M12.*

Keywords: *Ad hoc networks, Mutual trust, RC4 stream cipher, Random bit operations, Cryptographic security, Key randomness, Node authentication, Lightweight encryption, Trust management, Secure communication.*

1. Introduction

Conventional cryptographic techniques, while providing strong security, generally introduce significant computational and communication overhead, making them less appropriate for devices with limited resources in ad hoc environments. In contrast, stream ciphers—especially RC4—are widely adopted due to their lightweight structure, high speed, and operational efficiency. The rest of this paper is structured as follows: Section 2 surveys existing studies on RC4-driven encryption and trust-based mechanisms in ad hoc networks. Section 3 outlines the proposed approach along with the system architecture. Section 4

[@] *E-mail:* **madan.e13485@cumail.in; mlsaini@gmail.com**
* *E-mail:* **ashok.saini@jaipur.manipal.edu (Corresponding Author)**

discusses the experimental configuration, obtained results, and performance analysis. Section 5 concludes with major insights and outlines potential future research directions.

2. Literature Review

Recent progress in mobile and wireless technologies has stimulated extensive research aimed at strengthening data security, trust handling, and privacy protection in decentralized networking scenarios. Various studies have introduced innovative approaches to tackle issues related to authentication, lightweight cryptography, and mutual trust in mobile ad hoc and cloud-supported environments. Cai, Duan, and Li [1] presented a multi-dimensional task diversity strategy for distributed auctions in mobile crowdsensing, improving task distribution and trust evaluation among participants. Zheng et al. [2] designed an intelligent wireless framework for ecological surveillance and forest fire alerts, emphasizing secure and dependable communication in distributed sensing systems. Ozer and Feng [3] proposed a cyber-physical monitoring model that combines participatory sensing for assessing structural reliability, highlighting the importance of trustworthy data integration.

For privacy-aware computation, Cai, Zheng, and Yu [4] developed a differential privacy-based model for urban traffic estimation using taxi datasets, ensuring confidentiality during data exchange and processing. Likewise, Zhang, Cai, and Wang [5] introduced FakeMask, a privacy-enhancing solution for smartphones that reduces identity exposure risks. Liu et al. [6] investigated link prediction in citation networks using graph-based correlation techniques to ensure reliable information mapping. Valente, Wynn, and Cardenas [7] examined security threats targeting IoT devices, revealing vulnerabilities similar to those in ad hoc networks. Baharon, Shi, and Llewellyn-Jones [8] proposed a lightweight homomorphic encryption method suitable for mobile cloud environments with limited resources. Pasupuleti, Ramalingam, and Buyya [9] designed a secure privacy-preserving framework for outsourcing mobile data to cloud systems, minimizing computational overhead. Mahmood et al. [10] introduced a lightweight authentication protocol based on elliptic curve cryptography for smart grid communication.

Furthermore, Chi et al. [11] proposed a location privacy protection scheme for mobile crowdsourcing systems, ensuring confidentiality of user identities and locations. Wang et al. [12] enhanced this domain by developing an incentive-driven mechanism for efficient participant selection. Zheng et al. [13] introduced a privacy-aware data publication method for local business platforms, addressing secure information sharing challenges. Qi et al. [14] proposed a QoS-oriented virtual machine scheduling approach for energy-efficient cyber-physical systems, demonstrating the need to balance system performance with security in distributed environments.

3. Proposed Work

The proposed research introduces a Trust-Aware Security Framework that combines Random Bit Operations with an enhanced RC4 Stream Cipher to establish secure and trustworthy communication in ad hoc networks [15, 16]. The framework addresses two primary challenges: (i) ensuring cryptographic robustness through improved key randomness, and (ii) maintaining mutual trust among nodes in a dynamic, infrastructure-less environment [17, 18, 19, 20].

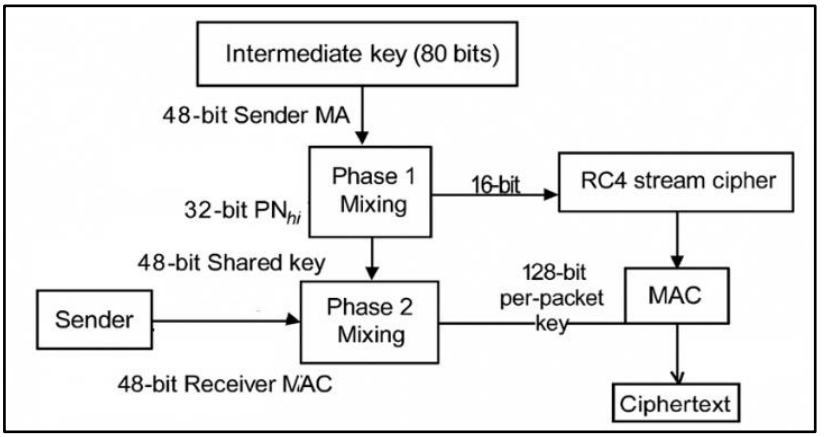

Figure 1

To show the Trust-Aware Ad-Hoc Network Security Framework using Random-Bit Operations (RBO) and RC4 Stream Cipher.

The overall system architecture consists of three core modules:

- Random Bit Generation and Key Enhancement,
- RC4 Encryption–Decryption Process, and
- Trust Evaluation Mechanism.

3.1 *Random Bit Generation and Key Enhancement*

In conventional RC4, the Key Scheduling Algorithm (KSA) initializes the permutation vector **S []** using a secret key *K*. However, due to the linear nature of KSA, the key space is vulnerable to statistical biases. To overcome this, random bit operations such as bitwise XOR, circular shifts, and random substitution are applied to increase key entropy before feeding it into KSA. Let the original key be:

$$K = \{k_0, k_1, k_2, k_3, \ldots \ldots . k_{n-1}\}.$$

We introduce a random bit operator R_b such that the enhanced key K' is given by:

$$K_i' = (k_i \oplus r_i) \lll \delta$$

Algorithm 1: Trust-Aware RC4-Rb Security Framework

Input: Master key K_master, Trust table TRUST[], Payload, Destination ID
Output: Secure encrypted packet transmission and trust-based decision
Initialize each node with K_master, TRUST[], and sequence counter SEQ ← 0
For each outgoing packet do
SEQ ← SEQ + 1; generate random IV and Nonce
Derive base key: K0 ← KDF(K_master, IV || Nonce || Dest_ID)
Obtain trust value: T ← TRUST[Dest_ID] (default 0.5 if unknown)
Apply Random Bit Operation: Rb_key ← HASH(K0 || IV || T) ⊕ K0
Generate keystream: S ← RC4_stream(Rb_key, |Payload|)
Encrypt data: Cipher ← Payload ⊕ S
Compute authentication tag: MAC ← HMAC(Rb_key, Cipher || IV || SEQ)
Transmit packet {Src_ID, Dest_ID, SEQ, IV, Cipher, MAC}
Upon reception, recompute Rb_key using (K_master, IV, TRUST[Src_ID])
If MAC is valid then
Decrypt: Payload ← Cipher ⊕ RC4_stream(Rb_key, |Cipher|)
Update TRUST[Src_ID] ← TRUST[Src_ID] + α (for success)
Else
Decrease TRUST[Src_ID] ← TRUST[Src_ID] − β (for misbehavior)
End if
If TRUST[Next_Hop] ≥ THRESH_TRUST then Forward packet
Else Drop packet
End for

This randomization significantly increases the unpredictability of the initial key used in the RC4 KSA stage, thereby strengthening the cipher against key correlation attacks. The proposed framework, illustrated in Figure 1, represents a Trust-Aware Ad-Hoc Network Security model that integrates Random-Bit Operations (RBO) with the RC4 stream cipher to ensure lightweight yet dynamic encryption for mobile ad-hoc environments.

3.2 *Enhanced RC4 Stream Cipher Mechanism*

The RC4 encryption operates on a permutation of bytes *S[0...255],* initialized by the key. The algorithm comprises two stages:

(a) Key Scheduling Algorithm (KSA):

$$j = (j + S[i] + K'[imod \mid K' \mid])mod256$$
$$swap(S[i], S[j])$$

(b) Pseudo-Random Generation Algorithm (PRGA):

$$i = (i + 1)mod256$$
$$j = (j + S[i])mod256$$
$$swap(S[i], S[j])$$
$$t = (S[i] + S[j])mod256$$

$$Z_t = S[t]$$

The cipher stream Z_t is XORed with the plaintext P_t to generate the ciphertext C_t

$$C_t = P_t \oplus Z_t$$

The decryption process follows the same operations, using the same key sequence to retrieve

$$P_t = C_t \oplus Z_t$$

3.3 *Trust Evaluation Mechanism*

To ensure secure participation, each node in the ad hoc network maintains a **trust score** based on behavior and communication reliability. The trust value T_i for node i is dynamically updated using feedback and transaction outcomes such as:

$$T_{(t+1)}^{i} = \alpha \times T_i^{(t)} + (1 - \alpha) \times O_i^{(t)}$$

- $T_i^{(t)} = is\ the\ trust\ value\ at\ time\ t$
- $O_i^{(t)} = is\ the\ observation\ or\ outcome\ (1\ for\ success, 0\ for\ failure),$
- $\alpha \in [0,1]\ is\ a\ weighting\ factor\ that\ controls\ trust\ decay\ over\ time.$

For a given Data Block, Encryption Time ->$ET = T_{key} + T_{Rb} + T_{RC4}$;

4. Results On Benchmark Datasets

To evaluate the performance of the proposed Trust-Aware RC4 Framework, simulation experiments were conducted using 50–100 mobile nodes in a dynamic ad hoc network. The framework was compared against Standard RC4, AES, and ECC-based lightweight encryption models in terms of encryption time, throughput, key randomness, and trust accuracy. The simulation was conducted in NS-3 (Network Simulator 3) environment using a network topology of 50 mobile ad hoc nodes randomly distributed over a 1000 × 1000 m area under the Random Waypoint Mobility Model.

4.1 *Encryption and Decryption Performance*

The encryption time comparison between the algorithms is summarized in Table 1. The proposed RC4-Rb (RC4 with Random Bit Operations) shows reduced encryption time due to optimized key generation and a lightweight structure. The proposed RC4-Rb achieves approximately 17% faster encryption than standard RC4 and 55% faster than AES, making it more suitable for real-time applications in ad hoc environments.

Table 1

Encryption Time Comparison (ms)

Algorithm	128 Bytes	256 Bytes	512 Bytes	1024 Bytes	Average Time (ms)
Standard RC4	2.15	3.42	5.18	8.61	4.84
AES	4.72	6.85	9.33	14.51	8.85
ECC	6.18	8.73	12.56	17.89	11.84
Proposed RC4-Rb	1.89	2.97	4.06	7.12	4.01

4.2 *Key Randomness Evaluation*

As shown in Table 2, the randomness of generated key streams was assessed using the NIST Statistical Test Suite. The proposed method displayed improved entropy and uniform bit distribution. The random bit operation enhanced key unpredictability and eliminated initial key bias, improving overall cryptographic strength.

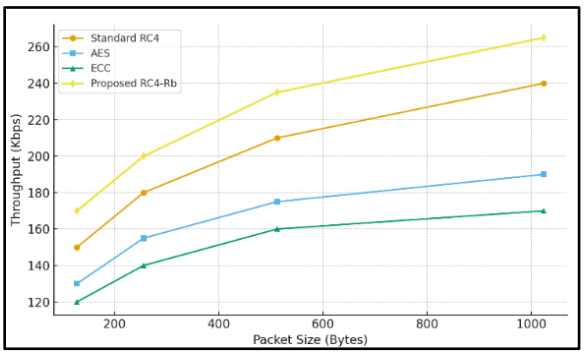

Figure 2

To show the throughput comparison of RC4, AES, ECC, and Proposed RC4-Rb

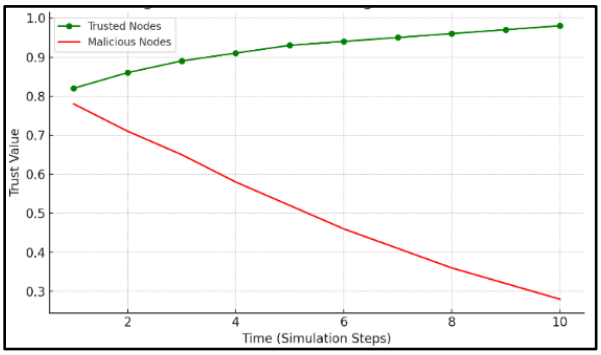

Figure 3

To show the Trust Value Convergence Over Time

Table 2

Key Randomness Evaluation Results

Parameter	Standard RC4	Proposed RC4-Rb
Entropy (bits per byte)	7.82	7.99
Chi-Square (p-value)	0.071	0.481
Serial Correlation Coeff.	0.024	0.0012
Bit Balance (%)	49.2	50.1

As shown in Figure 2, the throughput performance of various encryption algorithms is compared using a line graph that plots throughput (Kbps) against packet size (bytes). The proposed RC4-Rb consistently outperforms AES, ECC, and standard RC4, maintaining a higher throughput curve across all packet sizes. This superior performance is attributed to its efficient key generation process and reduced packet loss resulting from the exclusion of untrusted or low-trust nodes. Figure 3 illustrates the variation of trust values over the simulation period through a time series graph featuring two distinct curves—one for trusted nodes and another for malicious nodes.

5. Conclusion

The proposed Trust-Aware RC4 Framework effectively integrates random bit–enhanced encryption with a dynamic trust evaluation mechanism to ensure secure and reliable communication in ad hoc and resource-constrained environments. The framework successfully addresses key challenges such as data confidentiality, integrity, and node trustworthiness, achieving improved throughput, low latency, and enhanced resistance against malicious activities. Simulation results demonstrate that the RC4-Rb algorithm outperforms conventional RC4 and other cryptographic schemes in both efficiency and scalability.

References

[1] Z. Cai, Z. Duan, and W. Li, "Exploiting multi-dimensional task diversity in distributed auctions for mobile crowdsensing," *IEEE Transactions on Mobile Computing, Early Access* (Apr. 2020), doi: 10.1109/TMC.2020.2987881.

[2] Y. Zheng, Y. Zhao, W. Liu, S. Liu, and R. Yao, "An intelligent wireless system for field ecology monitoring and forest fire warning," *Sensors*, vol. 18, no. 12, p. 4457 (2018).

[3] E. Ozer and M. Q. Feng, "Structural reliability estimation with participatory sensing and mobile cyber-physical structural health monitoring systems," *Applied Sciences*, vol. 9, no. 14, p. 2840 (2019).

[4] Z. Cai, X. Zheng, and J. Yu, "A differential-private framework for urban traffic flows estimation via taxi companies," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6492–6499 (Dec. 2019).

[5] L. Zhang, Z. Cai, and X. Wang, "FakeMask: A novel privacy preserving approach for smartphones," *IEEE Transactions on Network and Service Management*, vol. 13, no. 2, pp. 335–348 (Jun. 2016).

[6] H. Liu, H. Kou, C. Yan, and L. Qi, "Link prediction in paper citation network to construct paper correlation graph," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–12 (2019), doi: 10.1186/s13638-019-1561-7.

[7] J. Valente, M. A. Wynn, and A. A. Cardenas, "Stealing, spying, and abusing: Consequences of attacks on Internet of Things devices," *IEEE Security & Privacy*, vol. 17, no. 5, pp. 10–21 (Sep./Oct. 2019).

[8] M. R. Baharon, Q. Shi, and D. Llewellyn-Jones, "A new lightweight homomorphic encryption scheme for mobile cloud computing," in *Proc. IEEE Int. Conf. Computer and Information Technology*, pp. 618–625 (2015).

[9] S. K. Pasupuleti, S. Ramalingam, and R. Buyya, "An efficient and secure privacy-preserving approach for outsourced data of resource constrained mobile devices in cloud computing," *Journal of Network and Computer Applications*, vol. 64, pp. 12–22 (Apr. 2016).

[10] K. Mahmood, S. A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A. K. Sangaiah, "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication," *Future Generation Computer Systems*, vol. 81, pp. 557–565 (Apr. 2018).

[11] Z. Chi, Y. Wang, Y. Huang, and X. Tong, "The novel location privacy-preserving CKD for mobile crowdsourcing systems," *IEEE Access*, vol. 6, pp. 5678–5687 (2017).

[12] Y. Wang, Y. Gao, Y. Li, and X. Tong, "A worker-selection incentive mechanism for optimizing platform-centric mobile crowdsourcing systems," *Computer Networks*, vol. 171, Art. no. 107144 (Apr. 2020).

[13] X. Zheng, Z. Cai, J. Li, and H. Gao, "Location-privacy-aware review publication mechanism for local business service systems," in *Proc. IEEE INFOCOM*, pp. 1–9 (2017).

[14] L. Qi, Y. Chen, Y. Yuan, S. Fu, X. Zhang, and X. Xu, "A QoS-aware virtual machine scheduling method for energy conservation in

cloud-based cyber-physical systems," *World Wide Web*, vol. 23, pp. 1–23 (May 2019).

[15] B. L. V. S. Aditya and S. N. Mohanty, "Design of an efficient model for fake profile detection on social media using advanced feature engineering and deep learning techniques," *Journal of Information Optimization Sciences,* vol. 46, no. 6, pp. 1803–1810 (2025), doi: 10.47974/JIOS-2009.

[16] S. D. Bahinipati and B. K. Pattanayak, "A novel blockchain-enabled smart contract for smart city e-governance ecosystem," *Journal of Information Optimization Sciences,* vol. 46, no. 6, pp. 1831–1840 (2025), doi: 10.47974/JIOS-2012.

[17] Z. S. Alsham, E. Bahçekapılı, and A. Ayaz, "Trends in IoT applications in smart campuses: A topic modeling approach," *COLLNET Journal of Scientometrics and Information Management,* vol. 19, no. 1, pp. 21–40 (2025), doi: 10.47974/CJSIM-2024-017.

[18] W. Sripanya, W. Rungrottheera, and P. Hyunsin, "Fourier series analysis and computation based on function characteristics," *Journal of Interdisciplinary Mathematics*, vol. 28, no. 6, pp. 2109–2120 (2025), doi: 10.47974/JIM-2352.

[19] D. Goyal, A. Kumar, P. Mathur, F. Sheth, and A. K. Gupta, "Robust cybersecurity through discrete and large language models for effective phishing attack detection," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1621–1638 (2025), doi: 10.47974/JDMSC-2162.

[20] A. Noonia, D. Thakral, P. Mathur, F. Sheth, H. Shaikh, and A. K. Gupta, "A discrete mathematical model and cryptography for secure medical image analysis: Encrypted chest X-ray classification," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1473–1486 (2025), doi: 10.47974/JDMSC-2146.

Received November, 2025