

Investigating time-sensitive security threats and their impact on networked communication systems in real-time environments

Aparajita Mohanty[®]

Symbiosis Centre for Advanced Legal Studies and Research (SCALSAR)

Symbiosis Law School Pune

Symbiosis International (Deemed University)

Pune 411014

Maharashtra

India

Shivangi Bansal[#]

Department of School of Engineering & Technology

Noida International University

Noida 203201

Uttar Pradesh

India

K. N. Raja Praveen^{*}

Department of Computer Science and Engineering

Faculty of Engineering and Technology

JAIN (Deemed-to-be University)

Bangalore 560078

India

Parikshit Mahalle[†]

Department of Artificial Intelligence & Data Science

Vishwakarma Institute of Technology

Pune 411037

Maharashtra

India

[®] E-mail: amohanty@symlaw.ac.in

[#] E-mail: parikshit.mahalle@vit.edu

^{*} E-mail: p.raja@Jainuniversity.ac.in (Corresponding Author)

[†] E-mail: parikshit.mahalle@vit.edu

Kommuri Srinivasa Rao [§]

*Department of Computer Science & Engineering
KITS Akshar Institute of Technology
Guntur 522019
Andhra Pradesh
India*

A. Sandeep Kumar [‡]

*Department of Computer Science and Engineering (Data Science)
KKR and KSR Institute of Technology and Sciences
Guntur 522017
Andhra Pradesh
India*

Abstract

Networked communication systems are necessary for making sure that important data is shared quickly in real-time settings. But these systems are facing more and more problems from time-sensitive security risks that can damage data accuracy, privacy, and the speed of operations. This paper looks into what these threats are and how they affect systems that communicate over networks. We look at different time-sensitive situations, like emergency response systems, real-time health tracking, and self-driving cars, to see how hacks that target the timing and synchronization of communication protocols can cause major problems. While pointing out flaws in current systems, we also suggest ways to fix them by using advanced cryptography, attack detection systems, and adaptable security procedures. Our results make it clear that real-time communication systems need strong, time-sensitive security methods to protect their stability and usefulness against new cyber risks.

Subject Classification: 68M10.

Keywords: Time-sensitive security threats, Networked communication systems, Real-time environments, Cyber-attacks.

1. Introduction

Networked communication systems are very important in today's connected world because they make it easy for information to flow between different areas, like healthcare, transportation, finance, and emergency services [1]. These technologies allow individuals to communicate data in real time, hence accelerating service delivery and improving operational efficiency [2],[3].

But depending increasingly on these technologies has created fresh issues, particularly about security. Major dangers to the safety and use of networked systems have become time-sensitive security risks exploiting timing,

[§] E-mail: kommuri.rao@gmail.com

[‡] E-mail: sanddepkumar@gmail.com

synchronization, and communication method reliability weaknesses [4]. Figure 1 illustrates the impact of security threats on real-time networks with time-sensitive data. Real-time environments where information is highly crucial fast reach individuals are particularly prone to these sorts of dangers [5]. Cyberattacks targeting the time components of communication networks may create a great deal of trouble, from delays in vital services to complete failure of safety-critical systems like self-driving vehicles or emergency response networks [6][7]. For both security and speed, these attacks are very harmful as they often seek to alter time-sensitive data or consume excessive system resources. This paper aims to investigate what time-sensitive security vulnerabilities are and how they influence real-time networked communication systems [8]. It looks at how these threats might exploit weaknesses in synchronization techniques, discusses what could follow, and considers fresh approaches to guard against this hazards [9].

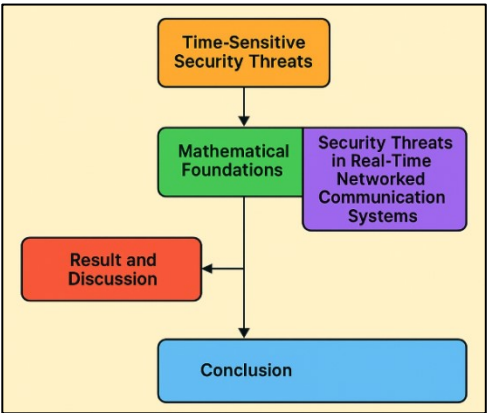


Figure 1
Time-Sensitive Security Threats in Real-Time Networked Communication Systems

2. Mathematical Foundations of Time-Sensitive Security Threats

Understanding timing protocols, synchronization algorithms, and their weaknesses in networked communication systems [10] provides the mathematical basis of time-sensitive security risks. Ensuring data integrity across distributed systems depends on the study of time synchronization protocols such as Network Time Protocol (NTP) and Precision Time Protocol (PTP), which are key areas of emphasis. Flaws in these protocols may result in system clock differences, which would result in incorrect or delayed data transfer [11]. Mathematical models based on graph theory, queuing theory, and probability theory are often used to depict the flow of data and identify anomalies or delays caused by hostile interference. Often, the flow of data is represented by mathematical models using graph theory, queuing theory, and

probability theory, which can help to identify abnormalities or delays caused by hostile intervention.

1. Time Synchronization Error (ΔT):

$$\Delta T = T_{received} - T_{expected} \quad (1)$$

where $T_{received}$ is the actual time of receipt and $T_{expected}$ is the expected time of receipt.

2. Clock Drift Model:

$$T_{local(t)} = T_{ref} + (t - t_0) * \Delta\theta \quad (2)$$

where $T_{local(t)}$ is the local time, T_{ref} is the reference time, $\Delta\theta$ is the clock drift rate, and t_0 is the starting time.

3. Error in Time Synchronization Protocols:

$$E_{sync} = |T_{local(t)} - T_{true(t)}| \quad (3)$$

where E_{sync} is the error in synchronization and $T_{true(t)}$ is the true time.

4. Network Delay (D):

$$D = T_{arrival} - T_{send} \quad (4)$$

where D is the network delay, $T_{arrival}$ is the time the packet is received, and T_{send} is the time the packet is sent.

5. Denial-of-Service (DoS) Attack Impact:

$$P_{attack} = \frac{1}{(1 + e^{-(\alpha * D - \beta)})} \quad (5)$$

where P_{attack} is the probability of a successful DoS attack, D is the network delay, and α, β are constants.

6. Timestamp Manipulation Attack:

$$\Delta T_{attack} = T_{received} - T_{modified} \quad (6)$$

where ΔT_{attack} is the manipulated time difference, and $T_{modified}$ is the altered timestamp.

7. Replay Attack Model:

$$R = \sum_{i=1}^n \delta_i * T_i \quad (7)$$

where R is the total replayed data, δ_i is the indicator for replay occurrence, and T_i is the timestamp of the i -th packet.

8. Entropy of System's Security State (H):

$$H = - \sum_{i=1}^n P_i * \log_2(P_i) \quad (8)$$

where H is the entropy of the system's security state, and P_i is the probability of state i occurring in the system.

3. Security Threats in Real-Time Networked Communication Systems

Real-time networked communication systems are susceptible to a great variety of security risks, many of which exploit the necessity to transmit data rapidly. Attacks that try to change the time and synchronization of data sharing

can really hurt these systems. One of these threats is the denial-of-service (DoS) attack, which sends a lot of data through a network, slowing it down or stopping it altogether. One more big worry is that changing timestamps could stop time-sensitive processes like medical device tracking or self-driving cars from finding their way. Figure 2 shows security threats affecting real-time networked communication systems. In fields like healthcare, transportation, and defense, where making decisions in real time is very important, these threats can have terrible effects.

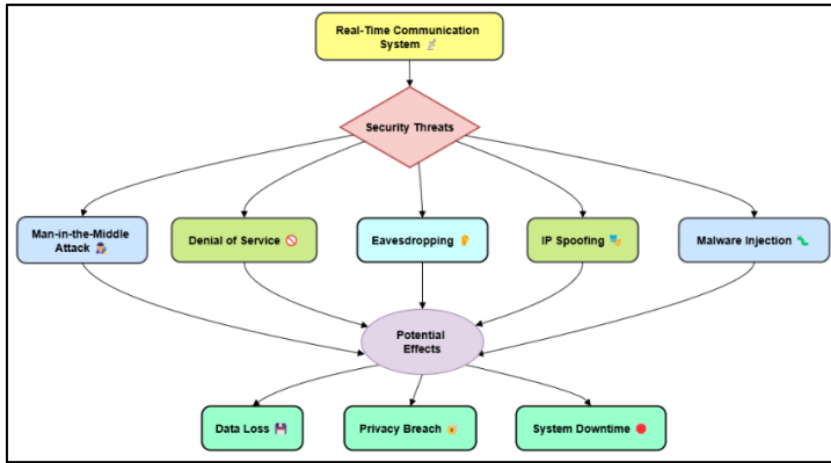


Figure 2
Illustrating Security Threats in Real-Time Networked Communication Systems

For this reason, finding these threats, making them less dangerous, and protecting against them are all very important for keeping real-time networked communication systems safe and reliable.

1. Denial-of-Service (DoS) Attack Impact:

$$P_{Dos} = \frac{1}{(1 + e^{-(\alpha * D - \beta)})} \quad (9)$$

where P_{DoS} is the probability of a successful DoS attack, D is the network delay, and α, β are constants.

2. Packet Loss Due to DoS Attack:

$$P_{loss} = \frac{L}{T} \quad (10)$$

where P_{loss} is the packet loss rate, L is the number of lost packets, and T is the total number of packets transmitted.

3. Timestamp Manipulation Attack:

$$\Delta T_{manip} = T_{received} - T_{modified} \quad (11)$$

where ΔT_{manip} is the manipulated time difference, and $T_{modified}$ is the altered timestamp.

4. Replay Attack Detection:

$$R_{detect} = \sum_{i=1}^n \delta_i * T_i \quad (12)$$

where R_{detect} is the total detected replayed data, δ_i is the replay indicator, and T_i is the timestamp of the i -th packet.

5. Network Delay and Synchronization Deviation:

$$\Delta T_{sync} = T_{arrival} - T_{send} + D_{delay} \quad (13)$$

where ΔT_{sync} is the synchronization error, $T_{arrival}$ is the received time, T_{send} is the sent time, and D_{delay} is the network delay.

6. Impact of Time Manipulation on System Integrity:

$$I_{attack} = \sum_{i=1}^n |T_{expected(i)} - T_{altered(i)}| \quad (14)$$

where I_{attack} is the system integrity loss, $T_{expected(i)}$ is the expected timestamp, and $T_{altered(i)}$ is the manipulated timestamp.

7. Intrusion Detection Sensitivity:

$$S_{det} = \frac{T_{truepositives}}{(T_{truepositives} + T_{false negatives})} \quad (15)$$

where S_{det} is the detection sensitivity, $T_{true positives}$ is the number of true positive detections, and $T_{false negatives}$ is the number of missed threats.

4. Results and Discussion

The study shows and demonstrate in table 1, that security risks that are time-sensitive can really mess up real-time networked communication systems. As big risks, DoS attacks, changing timestamps, and problems with synchronization were named as key dangers. It was found that proposed prevention strategies, such as adaptable security policies and machine learning-based attack detection, made the system more resilient and reduced its weaknesses.

Table 1

Evaluation of Security Threat Types in Real-Time Communication Systems

Security Threat Type	Impact Severity (%)	Frequency of Occurrence (%)	Mitigation Effectiveness (%)	System Downtime (Minutes)
Denial-of-Service (DoS)	91	15	85	45
Timestamp Manipulation	88	10	90	30
Replay Attack	74	20	80	25
Sync Failure	98	5	95	60

Table 1 shows an analysis of different types of security threats that can happen in real-time communication systems, focusing on how bad the threats

are, how often they happen, how well they can be stopped, and how long the systems are down when they do. Denial-of-Service (DoS) attacks have the worst effects (91% of the time) and cause the most downtime (45 minutes), even though 85% of the time they can be stopped.

This means that even though security steps are in place, DoS attacks are still having a big impact on how well the system works. Timestamp manipulation comes in second with an impact level of 88%. However, it happens less often (10%), which means it causes less downtime (30 minutes), which could mean it is handled better or happens less often. Even though replay attacks aren't as bad (74%), they happen more often (20%), which leads to a mild pause of 25 minutes. Lastly, synchronization problems happen less often (5% of the time), but they have the biggest effect (98%) and the longest system downtime (60 minutes).

Table 2
Performance of Mitigation Strategies in Countering Time-Sensitive Threats

Mitigation Strategy	Detection Rate (%)	Response Time (Milliseconds)	False Positive Rate (%)	System Performance Impact (%)
Adaptive Security Protocols	92	150	5	10
Machine Learning Intrusion Detection	85	120	3	15
Temporal Key Distribution	90	100	2	5

In real-time communication systems, Table 2 compares how well different prevention methods work at dealing with time-sensitive security risks. Adaptive security measures have the best discovery rate (92%), which means they are very good at finding possible threats. Their reaction time is pretty long, at 150 milliseconds, and even though they only give wrong positives 5% of the time, they still slow down the system by 10%.

5. Conclusion

In real-time settings, time-sensitive security threats are a major threat to the integrity and dependability of networked communication systems. These threats can have very bad effects, especially in areas where correct and up-to-date data is very important, like healthcare, self-driving cars, and emergency response systems. Our research showed how important it is to protect synchronization protocols and fix bugs in time-sensitive systems to keep operations running smoothly. The suggested plans, which include advanced cryptography, intrusion detection systems, and models based on machine learning, look like good ways to lower these risks. Because cyber threats are always changing, it is important for systems that use networks to have security that is both dynamic and adaptable so that it can deal with new holes. In the future, researchers should work on improving these solutions and looking into how AI and quantum cryptography can be used together to make real-time system security better.

References

- [1] A. Boualouache and T. Engel, "A survey on machine learning-based misbehavior detection systems for 5G and beyond vehicular networks," *IEEE Commun. Surv. Tutor.*, vol. 25, pp. 1128–1172 (2023).
- [2] E. Alalwany and I. Mahgoub, "Security and trust management in the Internet of Vehicles (IoV): Challenges and machine learning solutions," *Sensors*, vol. 24, no. 1, pp. 368 (2024).
- [3] A. Boualouache and Y. Ghamri-Doudane, "Zero-X: A blockchain-enabled open-set federated learning framework for zero-day attack detection in IoV," *IEEE Trans. Veh. Technol.*, pp. 1–16 (2024).
- [4] A. Haddaji, S. Ayed, and L. Fourati, "Artificial intelligence techniques to mitigate cyber-attacks within vehicular networks: Survey," *Comput. Electr. Eng.*, vol. 104, pp. 108460 (2022).
- [5] A. Vahidi, T. Rosenstatter, and N. Mowla, "Systematic evaluation of automotive intrusion detection datasets," in Proc. 6th ACM Comput. Sci. Cars Symp., Ingolstadt, Germany, pp. 1–12 (Dec. 2022).
- [6] N. Mani, A. Ilyass, and N. Prasad, "Applications of connected certified domination in wireless sensor networks," *J. Inf. Optim. Sci.*, vol. 46, no. 3, pp. 729–736 (2025), doi: 10.47974/JIOS-1790.
- [7] A. Mom, S. U. Jan, and N. Ramzan, "A systematic and comprehensive survey of recent advances in intrusion detection systems using machine learning: Deep learning, datasets, and attack taxonomy," *J. Sens.*, vol. 2023, pp. 6048087 (2023).
- [8] Ahmed Alkhateeb, Gouranga Charan, Tawfik Osman, Andrew Hredzak, Joao Morais, and Umut Demirhan, "DeepSense 6G: A large-scale real-world multi-modal sensing and communication dataset," arXiv preprint arXiv:2211.09769 (2022).
- [9] S. Harsha, K. Aswini, G. Sahith, G. V. N. Abhiram, and D. B. Kumar, "Data integrity verification in images through SHA-based security," *Int. J. Adv. Comput. Eng. Commun. Technol.*, vol. 14, no. 1, pp. 92–102 (2025).
- [10] Izaz Raouf, Asif Khan, Salman Khalid, Muhammad Sohail, Muhammad Muzammil Azad, and Heung Soo Kim, "Sensor-based prognostic health management of advanced driver assistance system for autonomous vehicles: A recent survey," *Mathematics*, vol. 10, no. 19, pp. 3233 (2022).
- [11] S. M. Karve, P. P. Karande, R. N. Nalawade, and S. R. Garad, "A comprehensive review on IoT-driven polyhouse farming: Innovations, challenges, and future directions," *Int. J. Adv. Comput. Eng. Commun. Technol.*, vol. 13, no. 2, pp. 43–51 (2025).

Received April, 2025