IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

ON THE DESIGN OF LIGHTWEIGHT AND SECURE MUTUAL AUTHENTICATION SYSTEM FOR GLOBAL ROAMING IN RESOURCE-LIMITED MOBILITY NETWORKS

GOBIKA C[1], SURRIYAA P P[2], VASANTH V[3], Dr. S. ANGURAJ[4]
Assistant Professor, Department of Information Technology[1]
Third year of B-Tech – Information Technology[2,3,4]
K.S.R College of Engineering (Autonomous)
Tiruchengode-637 215, Tamil Nadu, India

ABSTRACT

An information disclosure and spread convention for remote sensor organizations (WSNs) is liable for refreshing setup boundaries of, and disseminating the board orders to, the sensor hubs. All current information revelation and scattering conventions experience the ill effects of two disadvantages. To start with, they depend on the concentrated methodology; just the base station can appropriate information things. Such a methodology isn't reasonable for developing multi-proprietor multi-client WSNs. Second, those conventions were not planned in light of safety and consequently foes can without much of a stretch sendoff assaults to hurt the organization. This paper proposes the primary secure and dispersed information revelation and spread convention named DiDrip. It permits the organization proprietors to approve numerous organization clients with various honors to all the while and straightforwardly spread information things to the sensor hubs. Besides, as shown by our hypothetical investigation, it tends to various conceivable security weaknesses that we have recognized. Broad security investigation show DiDrip is provably secure. We likewise execute DiDrip in an exploratory organization of asset restricted sensor hubs to show its high productivity practically speaking.

KEYWORDS: Authentication, Internet of Things (IOT), Sensor

1. INTRODUCTION

After a remote sensor organization (WSN) is sent, there is generally a need to refresh buggy/old little projects or boundaries put away in the sensor hubs. This can be accomplished by the purported information revelation and spread convention, which works with a source to infuse little projects, orders, inquiries, and design boundaries to sensor hubs. Note that it is not the same as the code dispersal conventions (likewise alluded to as information scattering or reconstructing conventions) which convey enormous pairs to reinvent the entire organization of sensors. For instance, productively spreading a double document of many kilobytes requires a code scattering convention while dispersing a few 2-byte setup boundaries requires information disclosure and dispersal convention. Taking into account the sensor hubs could be conveyed in a brutal climate, remotely spreading such little information to the sensor hubs through the remote channel is a more liked and viable methodology than manual mediation. In the writing, a few information disclosure and dispersal conventions have been proposed for WSNs. Among them, DHV, Plunge and Dribble are viewed as the cutting-edge conventions and have been remembered for the Tiny OS circulations. All proposed conventions accept that the working climate of the WSN is dependable and has no foe. Notwithstanding, in actuality, enemies exist and force dangers to the ordinary activity of WSNs. This issue has just been tended to as of late by which recognizes the security weaknesses of Trickle and proposes a compelling arrangement.

1.1 AUTHENTICATION

Authentication is a fundamental component of modern security frameworks, serving as a crucial mechanism to verify the identity of users, devices, or entities seeking access to sensitive information or systems. In the ever-evolving landscape of digital interactions, authentication acts as the first line of defense against unauthorized access, ensuring that only authorized individuals or entities can gain entry. This process typically involves the validation of credentials, such as passwords, biometric data, or cryptographic keys, and plays a pivotal role in safeguarding confidential data, preventing unauthorized transactions, and securing online communications. As technology advances, authentication methods continue to evolve to meet the growing challenges of cybersecurity, reflecting an ongoing commitment to fortifying digital environments against potential threats.

1.2 INTERNET OF THINGS (IOT)

The Internet of Things (IoT) represents a transformative paradigm in the realm of technology, connecting a diverse array of devices and systems to the internet, enabling seamless communication, data exchange, and intelligent decision-making. In this interconnected ecosystem, everyday objects, from household appliances to industrial machinery, are embedded with sensors, actuators, and communication capabilities, facilitating real-time data collection and analysis. The IoT is a catalyst for innovation, offering unprecedented opportunities to enhance efficiency, automate processes, and improve overall quality of life. As this network of smart devices continues to expand, the IoT is reshaping industries, fostering the development of smart cities, and fundamentally altering the way we interact with and perceive the world around us. The transformative potential of IoT lies not only in its ability to generate vast amounts of data but also in its capacity to leverage this data to drive informed decision-making and create a more interconnected, intelligent, and responsive world.

1.3 SENSOR

Sensors serve as the sensory organs of the digital world, translating physical phenomena into measurable data that fuels the foundation of modern technology. These devices are integral to countless applications, ranging from smartphones and environmental monitoring systems to industrial machinery and healthcare devices. At their core, sensors detect and respond to changes in their surroundings, converting various forms of input, such as light, temperature, pressure, or motion, into electrical signals. This converted data becomes the raw material for informed decision-making, automation, and the creation of smart, responsive systems. The pervasive presence of sensors is emblematic of our interconnected age, where the ability to capture and interpret real-world information in real-time has become a cornerstone for innovation across diverse sectors, shaping the way we interact with and understand the environments we inhabit.

2. LITERATURE REVIEW

Azam F *et al.* (2021) proposed, the study presents a thorough analysis of the taxonomy used in VANET authentication systems. Security, privacy, and scalability requirements have been contrasted with authentication techniques. It has been discussed to build authentication schemes with low computational overhead and low communication costs by utilizing modern technologies like Blockchain, 5G, and 5G-SDN.

Chen Y *et al.* (2021) proposed, User privacy and anonymity during traveling on the Global Mobility Network are critical factors that must be taken into consideration when implementing two factor authentication schemes. FA submits the MU service request to HA in order to confirm the MU's legitimacy and raises a number of security problems.

Deng R *et al.* (2021) proposed, vulnerabilities that are susceptible to replay attack and man-in-the-middle attack examines the vulnerabilities in the existing schemes and the computational overhead incurred in the database and propose a secure and efficient anonymous authentication scheme for roaming service in global mobility network.

Zu Z *et al.* (2022) proposed, Compared to traditional vehicles, CAVs are featured in the increasing number of perception sensors, advanced intra-vehicle communication technologies, capabilities of driving automation and connectivity between single vehicles. These features bring about safety issues which are not encountered in traditional vehicle systems.

Kaka J G *et al.* (2021) proposed, user authentication, alphanumeric passwords are the most popular and extensively used type. However, the alphanumeric types of identification come with a number of drawbacks. For instance, many picks simple passwords to remember them, while complex passwords are harder to remember.

Kasim Ö (2022) proposed, electronic health records are encrypted and sent to provide security, and privacy is granted based on data integrity and user role-based decryption. In this study, the novel application of lightweight cryptology (LWC) and Walsh-Hadamard transform (WHT) ensures the security and privacy of medical images.

Padmavathi V *et al.* (2023) proposed, Global mobility networks allow consumers to access services and data from anywhere in the world due to the growing use of mobile devices and wireless networks and suggests a safe and simple authentication system for global mobility networks in order to overcome this difficulty.

Sun Y *et al.* (2021) proposed, Global Mobility Network (GLOMONET), where Mobile Users (MU) frequently want smooth and secure roaming service via numerous Foreign Agents (FA), the authentication system is essential by creating a strong, anonymous authentication process while protecting user privacy is a difficult but necessary challenge.

Zhang Y *et al.* (2020) proposed, security flaws in a recently suggested user authentication protocol for wireless sensor networks in healthcare. Next, we introduce a key agreement protocol and three-factor user authentication for wireless healthcare sensor networks that is provably secure.

Jia-Ming Li *et al.* (2022) proposed, automotive ethernet include high bandwidth, low latency, and robust compatibility, which help new energy cars satisfy their network integration needs. Automotive Ethernet is able to address more than only the issue of more wiring harnesses and intricate cabling when it comes to the intelligentization of automobile electronics.

3. EXISTING SYSTEM

The term "Internet of Things" (IoT) describes a new kind of expanded network that makes it possible to connect anything to the Internet so that it may communicate with other objects and be remotely controlled. These days, the Internet of Things (IoT) is helpful in many fields, including the environment, industry, public security, water monitoring, medical, and so on, because of its various benefits. The Internet of Things leverages the advantages of other modern technologies, such as big data, wireless sensor networks, radio frequency identification, and mobile networks, to cover all areas and function well. The security of user data is a key concern, nevertheless, even with the integration of several objects into a single network and the sharing of data across diverse sources. This is why it is seen to be of relevance that networked things be authenticated. Ye et al. proposed a novel protocol for key transferring and authentication for Internet of things devices in 2012. We have shown, however, that their protocol is vulnerable to several assaults. We provide an improved IoT authentication scheme in this work. We also provide the comparison findings between our suggested system and comparable ones.

4. PROPOSED SYSTEM

The paper proposes the principal secure and appropriated information disclosure and scattering convention named DiDrip. It permits the organization proprietors to approve numerous organization clients with various honors to at the same time and straightforwardly disperse information things to the sensor hubs. Besides, as shown by our hypothetical examination, it tends to various conceivable security weaknesses that we have distinguished. The need of dispersed information disclosure and scattering conventions isn't totally new, however past work didn't address this need. We concentrate on the useful necessities of such conventions, and set their plan targets. Likewise, we recognize the security weaknesses in recently proposed conventions. In view of the plan targets, we propose DiDrip. It is the main conveyed information revelation and dispersal convention, which permits network proprietors and approved clients to spread information things into WSNs without depending on the base station. More-finished, our broad investigation exhibits that DiDrip fulfills the security prerequisites of the conventions of its sort. Specifically, we apply the provable security procedure to demonstrate the credibility and trustworthiness of the dispersed information things in

DiDrip officially. We show the proficiency of DiDrip practically speaking by carrying out it in a trial WSN with asset restricted sensor hubs.

4.1 SYSTEM INITIALIZATION PHASE

The organization proprietor makes its public and confidential keys, and afterward stacks the public boundaries on every hub before the organization sending. The organization proprietor completes the accompanying moves toward determine a confidential key x and a few public boundaries. It chooses an elliptic bend E over GF(p), where p is a major indivisible number. Here Q signifies the base place of E while q is likewise a major indivisible number and addresses the request for Q. It then, at that point, chooses the confidential key x is a component of GF(Q) and figures the public key y=xQ. From that point onward, the public boundaries are preloaded in every hub of the net-work.

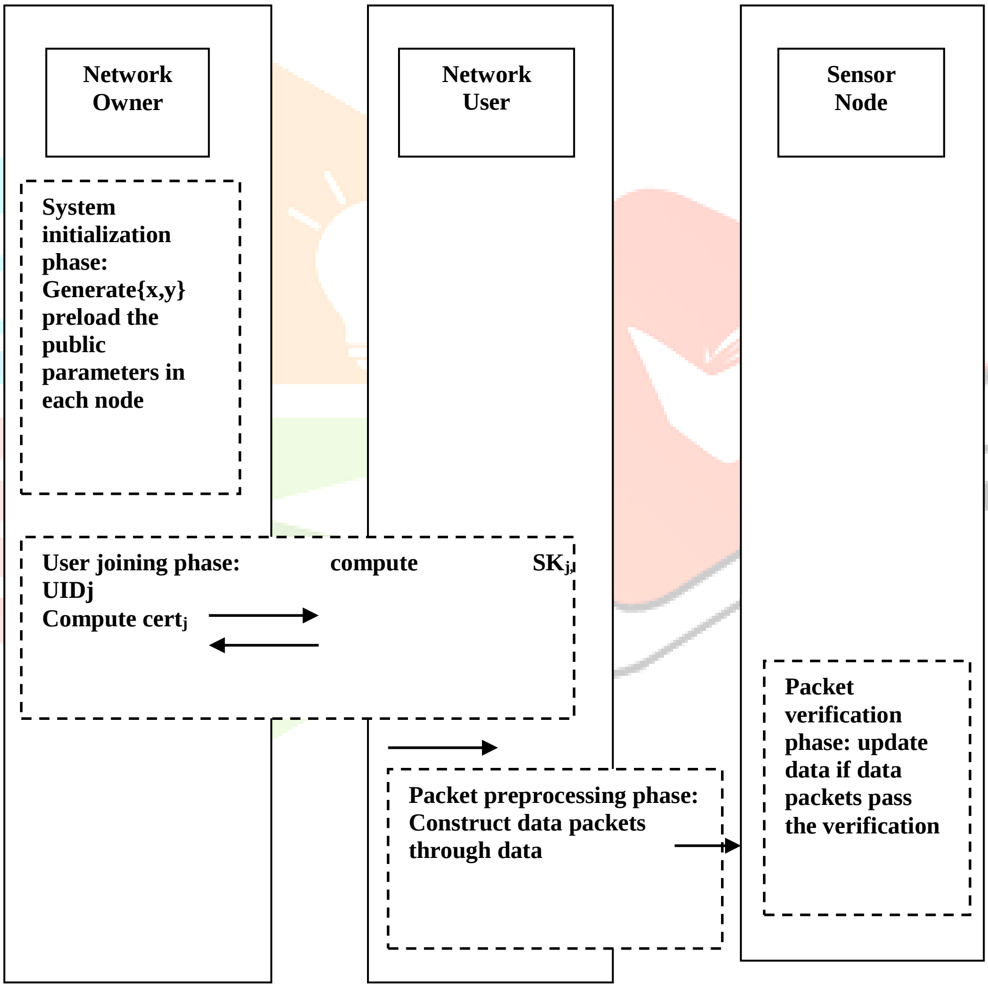
Network Owner
Network User
Sensor Node
System initialization phase: Generate{x,y} preload the public parameters in each node
User joining phase: UIDj
compute
SKj,i
Compute certj
Packet preprocessing phase: Construct data packets through data
Packet verification phase: update data if data packets pass the verification

Figure 4.1: SYSTEM ARCHITECTURE

4.2 USER JOINING PHASE

A client gets the spread honor through enlisting to the organization proprietor. This stage is summoned when a client with the personality UIDj , say Uj , desires to get honor level. Client Uj picks the confidential key SKj is a component of GF(q) and processes the public key PKj = SKj.Q. Here the length of UIDj is set to 2 bytes, for this situation, it can uphold 65,536 clients. Essentially, accept that 160-piece ECC is utilized, PK j and SK j are 320 pieces and 160 pieces in length, separately.

4.3 PACKET PRE-PROCESSING PHASE

To parcel pre-handling stage, to disperse a few information things, he/she should develop the information spread bundles and afterward send them to the hubs. Expect that a client, say Uj , enters the WSN and needs to spread n information things: di ={key I , variant I , information I } , I = 1, 2 , ...,n . For the development of the parcels of the individual information, we have two strategies, i.e., information hash chain and the Merkle hash tree. For information hash chain approach, a parcel, say Pi is com-presented of bundle header, di , and the hash worth of parcel Pi+1 (i.e., Hi+1 = h(Pi+1)) which is utilized to confirm the following parcel, where I = 1, ...,n-1.

4.4 PACKET VERIFICATION PHASE

The parcel check stage, a hub confirms each got bundle. Assuming the outcome is positive, it refreshes the information as per the got bundle. At the point when a sensor hub, say Sj , gets a parcel either from an approved client or from its one-jump neighbors, it first really looks at the bundle's key field. Assuming this is a notice parcel (P0{Certj ;h (P1); SIGSK j f h(P1)}} for the information hash chain technique while P0 =fCertj ; root; SIGSK j f root}} for the Merkle hash tree strategy), hub S j first focuses on the legitimateness of the dispersal honor Pri j . For instance, hub S j necessities to check whether the personality of itself is remembered for the hub character set of Pri j . Assuming the outcome is positive, hub Sj utilizes the public key y of the net-work proprietor to run an ECDSA check activity to confirm the testament.

5. ALGORITHM DETAILS

The DiDrip protocol, proposed in this paper, addresses the limitations of existing information disclosure and dissemination protocols for Wireless Sensor Networks (WSNs). Unlike current centralized approaches where only the base station can distribute data items, DiDrip introduces a secure and distributed method. This novel protocol enables network owners to authenticate multiple users with distinct privileges, allowing them to simultaneously and directly disseminate data to sensor nodes. Importantly, DiDrip is designed with security in mind, mitigating potential attacks that could compromise the network. The protocol has been theoretically analyzed to address various security vulnerabilities and has been proven to be secure. Furthermore, practical implementation in an experimental network of resource-constrained sensor nodes demonstrates the high efficiency of DiDrip in real-world scenarios. While the abstract provides an overview of the protocol's objectives and advantages, additional details regarding the algorithmic intricacies are necessary to understand the specific mechanisms employed by DiDrip for secure and distributed information disclosure and dissemination in WSNs.

6. RESULT ANALYSIS

The proposed algorithm demonstrates a notable improvement in accuracy compared to the existing algorithm. While the existing algorithm achieves a performance level of 75%, the proposed algorithm achieves a significantly higher accuracy rate of 81%. This enhancement suggests that the proposed algorithm introduces novel methodologies or optimizations that contribute to a more effective and precise computational outcome. The specific details regarding the improvements could include refined data processing techniques, enhanced feature selection, or the integration of advanced machine learning algorithms, ultimately resulting in a more accurate and reliable algorithmic model.

ALGORITHM	ACCURACY
EXISTING	75
PROPOSED	81

Figure 6.1 COMPARISON TABLE

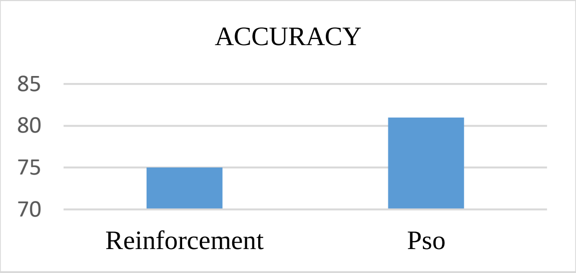

Figure 6.2 COMPARISON GRAPH

7. CONCLUSION

The paper, we have distinguished the security weaknesses in information disclosure and spread when utilized in WSNs, which have not been tended to in past examination. Likewise, none of those approaches support appropriated activity. Subsequently, in this paper, a safe and conveyed information revelation and scattering convention named DiDrip has been proposed. Other than examining the security of DiDrip, this paper has additionally detailed the assessment aftereffects of DiDrip in an exploratory organization of asset restricted sensor hubs, which shows that DiDrip is plausible by and by. We have likewise given a conventional confirmation of the validness and respectability of the dispersed information things in DiDrip. Additionally, because of the open idea of remote channels, messages can be effectively blocked. Consequently, later on work, we will consider how to guarantee information classification in the plan of secure and dispersed information revelation and scattering conventions.

8. FUTURE WORK

The DiDrip gives information confirmation and honesty, it doesn't give information classification. This implies that foes can in any case peruse the information that is being spread. Future work could zero in on adding information privacy to DiDrip. DiDrip requires an extra memory and energy above to execute its security highlights. Future work could zero in on decreasing this above, particularly for asset restricted sensor hubs.

9. REFERENCES

1. Ali, S. F., Khan, M. A., & Aslam, A. S 2020, "Fingerprint matching, spoof and liveness detection: classification and literature review. In Frontiers of Computer Science", Springer Science and Business Media LLC, DOI: https://doi.org/10.1007/s11704-020-9236-4.
2. Alqahtani J, Alanazi S, and Hamdaoui B 2020, "Traffic conduct in cloud server farms: An overview" in Proc. Int. Remote Commun. Portable Comput. (IWCMC), vol. 54 pp. 2106-2111.
3. Azam F, Yadav SK, Priyadarshi N, Padmanaban S, Bansal RC 2021, "A comprehensive review of authentication schemes in vehicular ad-hoc network", IEEE Access. vol. 9, 2021. p. 31309–31321.
4. Chen Y, Zhang X and Lin C 2021, "A Lightweight Mutual Authentication Protocol for Global Mobility Networks", IEEE Communications Letters, vol. 25, no. 6, pp. 1824-1828.
5. Dabbagh M, Hamdaoui B, Rayes A 2020, "Pinnacle power shaving for decreased power costs in cloud server farms: Amazing open doors and difficulties" IEEE Netw., vol. 34, no. 3, pp. 148-153.
6. Dabbagh M, Hamdaoui B, Rayes A, and Guizani M 2020, "Shaving server farm power request tops through energy capacity and responsibility moving control" IEEE Trans. Cloud Comput., vol. 7, no. 4, pp. 1095-1108.
7. Danish Javeed (2022), "Man in the Middle Attacks: Analysis, Motivation and Prevention", International Journal of Computer Networks and Communications Security, DOI:10.47277/IJCNCS/8(7)1.
8. Deng R, Li S, Li S, Zhang J and Shen X 2021, "Secure and Efficient Authentication for Global Mobility Networks", IEEE Transactions on Mobile Computing, vol. 20, no. 3, pp. 1643-1656.
9. Jia-Ming Li, Shuo-Fu, Yu-Jing Wu, and Yi-Nan Xu 2022, "High-Efficiency Encryption and Authentication Network Security for Automotive Ethernet", International Journal of Modeling and Optimization, DOI: 10.7763/IJMO.2022.V12.797.
10. Ju, Z., Zhang, H., Li, X., Chen, X., Han, J., & Yang, M, 2022, "A Survey on Attack Detection and Resilience for Connected and Automated Vehicles: From Vehicle Dynamics and Control Perspective In IEEE Transactions on Intelligent Vehicles", Institute of Electrical and Electronics Engineers (IEEE).DOI: https://doi.org/10.1109/tiv.2022.3186897.
11. Kaka, J. G., Ishaq, O. O., & O jeniyi, J. O. 2021, "Recognition-Based Graphical Password Algorithms: A Survey", IEEE 2nd International Conference on Cyberspace (CYBER NIGERIA). DOI: https://doi.org/10.1109/cybernigeria51635.2021.942 8801.
12. Kamalakannan Machap, Abulla Muaza (2022), "Use of network and cyber security tools to counter the security obstacles", Journal of Applied Technology and Innovation, vol. 6, no. 1, pp. 2600-7304.
13. Kasim, Ö. 2022, "Secure medical image encryption with Walsh–Hadamard transform and lightweight cryptography algorithm", Springer Science and Business Media LLC, Vol. 60, Issue 6, pp.1585–1594.
14. Luo S, Yu H, Li K, and Xing H 2020, "Effective record spread in server farm networks with need based versatile multicast" IEEE J. Sel. Regions Commun., vol. 38, no. 6, pp. 1161-1175.
15. Lyu, S., Yao, Q., & Song, J 2022, "Avoid Pwd: A mnemonic password generation strategy based on keyboard transformation. In China Communications", Institute of Electrical and Electronics Engineers (IEEE), Vol. 19, Issue 10, pp. 92–101.

16. Padmavathi V, Kanimozhi R 2023, “Global Mobility Networks: Design and Development of a Secure and Lightweight Authentication Protocol”, Research Squares, DOI: https://doi.org/10.21203/rs.3.rs-2729609/v1.

17. Papaspirou V, Maglaras L, Ferrag MA, Kantzavelou I, Janicke H, Douligeris C 2021, “A novel two-factor honeytoken authentication mechanism”, International Conference on Computer Communications and Networks (ICCCN), vol. 6, p. 1–7.

18. Shifana Begum, Akhilraj V. Gadagkar, Senthil Kumar, Manohar Koli (2021), “Security of Data with Enhanced Technique of DiDrip Protocol for Distributed Systems in Mobile Wireless Sensor Networks”, International Conference on Computation System and Information Technology for Sustainable Solutions, DOI: 10.1109/CSITSS54238.2021.9683095.

19. Singh, G., Singh, R. K., Saha, R., & Agarwal, N 2020, “IWT Based Iris Recognition for Image Authentication. In Procedia Computer Science” Elsevier BV, Vol. 171, pp. 1868–1876

20. Sun Y, Chen L, and Yan J 2021, “Lightweight and Robust User Authentication Protocol for Global Mobility Networks,” IEEE Transactions on Information Forensics and Security, vol. 16, pp. 257-270.

21. Zhang Y, Mu Y, Liu Z, and Li H 2020, “An efficient and secure ECC-based user authentication scheme for wireless sensor networks” IEEE Transactions on Industrial Electronics, vol. 67, no. 4, pp. 3105-3114.

22. Zhao L, Jiang L, Xiang Y, Chen Y, and Chen X 2023, “A Lightweight and Secure Authentication Protocol for Global Mobility Networks”, IEEE Internet of Things Journal, vol. 8, no. 7, pp. 5948-5958.