Efficient Measuring Secure Multi-Factor User Authentication Schemes For Wireless Sensor Networks

S.Gowri,A.Sivasankari,M.Kamarunisha

**Department of computer Applications,Dhanalakshmi Srinivasan College of Arts and Science for Women,,Perambalur , 621 212, Tamilnadu, , India.*

Email: gowris1255@gmail.com(Gowri s) Corresponding author: Gowri s

Abstract:- Many ideas have been put out, but the vast majority of them have been shown to be unsafe, and the same mistakes are repeated. Hub catch and brilliant card tragedy attacks are two of the most generally publicised security breaches. The prior has been extensively discussed in the literature, whereas little attention has been paid to the attacks on the hub. This is a huge step forward in the investigation of hub catch attacks against WSNs' multiple client verification plans. Hub catch attacks may be broken down into 10 various types based on the target's strengths or vulnerabilities that are exploited in the attack. At this stage, we examine 11 common weak conventions and offer corresponding defences for each kind of attack. Finally, we have the opportunity to lead a huge scope relative estimate of 61 agent client validation plans for WSNs under our all-inclusive evaluation standards. An understanding of hub catch attacks might be helpful in designing safe client verification procedures for WSNs.

Keywords: User authentication; node capture attacks; wireless sensor networks

I. INTRODUCTION

WSNs were born out of the need to remotely control, investigate, screen, and manage an unattended environment. Wireless sensor networks (WSNs) have a wide variety of applications because of their ubiquitous nature and easy design. There are a wide range of uses for WSNs, including but not limited to assessing the health and climate of a given area, monitoring military operations, and preventing the spread of natural, man-made, or nuclear risks in the area. In this way, remote monitoring of home and building security, as well as monitoring of health and safety through machines and crisis medical consideration, can be accomplished for a wide range of purposes, such as controlling traffic, monitoring combat zones, agrarian use estimation of seismic movement, producing in plants, natural life checking, temperature and humidity control in historical centres as well as so on. Because they enable the deployment of sensor networks in previously out-of-reach places, WSNs have been essential in bringing down the cost of infrastructure deployment. As a result, the range of applications has grown to the point where working with fixed sensor groups was formerly outside the realm of possibility [1]-[5].

A remote sensor network is a well-organized system that is capable of collecting, combining, and transmitting data at will. In order to grasp the "pervasive registration" mode, it brings together intelligent data and the real world. Smaller sensor hubs with limited battery power and calculating capacity may be used in untended areas, such as living spaces, medical services, farming, battle zones, and ecological monitoring. WSNs can also be used to monitor the environment. Hubs detect the weather and relay their findings to a nearby passage hub through remote channels, where they may be accessed by outside customers. In this way, WSNs may be used in a broad range of scenarios including city management, crisis medical consideration, temperature and mugginess monitoring in farming, untamed life checking, antiterrorism, military protection and more. No matter how they are conveyed, an opponent may spy, infiltrate, redirect, and manipulate the communications delivered over the remote channel because to the nature of remote correspondence and the fragility of its transmission. There has been a lot of work done on lower levels like interface and organisation but it is still necessary to create common validation plans with key arrangement in the application layer to prevent unauthorised access to the sensor hub [6]-[10].

The development of remote sensor networks is increasing at a rapid pace. There are a variety of ways in which WSN innovation and norms are examined each year, including both private and public research. Since recently, botnet attacks, along with the Internet of Things, have impacted various domain name workers and online service providers. Call-backs are made to all IoT devices that have been affected by botnet attacks. As a result, in today's WSN and IoT environments, security and reliability are viewed as essential.

Remote sensor networks shown are made of small sensors that assist each other out in a random way. Consolidated arrangement, arbitrary transmitting, variable geography, limited transfer speed, portable or stilled sensors, and self-configuration sensor hubs are some of the characteristics of a sensor network Sensors in difficult-to-reach locations are used to obtain this data in the current scenario. There are no mistakes in this information, and it doesn't change throughout transmission. Rivals of WSN may negotiate with the organisation using a variety of freedoms granted by WSN. Because of the nature of transmission and the vcd's flexibility, the organisation is exposed to a wide range of risks. It is essential that the Internet Integrated Sensor Network is capable of providing security from a variety of threats and attacks. Organizations that provide security services have a good opportunity as the network connecting the Internet, sensors, and clever devices grows [11]-[15].

II. RELATED WORKS

In [1], Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, Mauro Conti et al. report a study. Clients must be able to get continuous data from detecting hubs for a given application in a typical IoT organising atmosphere in order to benefit from HIoTN. "Client Validated Key Administration Convention" is the name of a new three-factor authentication scheme for HIoTNs that this article focuses on. Client shrewd card, secret word, and individual biometrics are all used in UAKMP. The plan's security is examined using the widely used Real-Or-Random model, casual security, and appropriate security verification using the well accepted AVISPA instrument. Unreservedly secret key and biometric updates, client anonymity and detecting hub obscurity are only a few of the advantages of UAKMP above other similar systems that are already in use. The UAKMP, on the other hand, is almost equal in both calculation and communication expenses when compared to current programmes.

[2] JianghongWei, Xuexian Hu, Wenfen Liu t al introduce the telecare medication data framework, which supports or enhances medical care delivery administrations in [2]. In order to ensure the safety of patients' personal information, such as their phone number or medical record number, a secure verification strategy will be implemented. For the telecare medication data framework, Wu et al. recently presented a clever card-based secret word confirmation scheme. As a result, He et al. brought up the fact that Wu et al's. approach couldn't evade pantomime and insider attacks, and then presented another method. They both fall short of meeting the two-factor authentication requirements that clever card-based secret word verification methods should meet. The revised telecare medication data framework verification plot also meets the security requirements of two-factor authentication and is also more effective, according to our findings.

Presents Shipra Kumari, Hari Om et al[3] .'s work Coal mine shafts, in particular, are a good place to look for the security and prerequisites of remote sensor networks in order to ensure the well-being of workers. They assist in reducing risks while enhancing efficiency by ensuring that the kinds of equipment and subsurface conditions are properly checked. Colliery specialists need to know more about a WSN's climate sensor in mines since even a tiny error might cause severe human setbacks and massive asset destruction, which could lead to massive financial losses. It is important to use the sensors' limited battery power wisely while processing the data they collect. For WSN security, we provide a verification convention that verifies the clients and mechanical sensors. Lightweight capacity and simplicity of transmission are all that are needed to conserve sensors' batteries.

This article by Mohammad Wazid, Ashok Kumar Das, Neeraj Kumar, and others can be found at [4]. Smart life, savvy health, and smart transportation are all examples of how Information and Communication Technology has been put to use. Customers/occupants may use ICT to control various smart sensor devices in their homes in a "bright home," which is often the most popular of all these applications. Sophisticated devices and clients, on the other hand, communicate across a fragile communication channel, namely, the Internet. There may be a variety of attacks, such as a customer, door hub, and savvy gadget pantomime assault, as well as a preferred insider attack on a clever home company. Information transmitted by clever devices may be used to get access to an illegitimate client in this case. For the reasons outlined above, the great majority of existing designs for remote client verification in a smart home context are insecure. As a result, a smart home company must devise a secure remote client validation strategy to allow only those clients who have been allowed access to the innovative devices. In this study, we present a secure remote client verification scheme that will help to alleviate some of the concerns raised in the preceding section. Using just single-direction hash capacity, bitwise XOR activities and symmetric encryptions/decoding, the suggested plot is useful for asset-constrained smart gadgets with limited resources. According to widely accepted Real-Or-Random paradigm, the plan's security is shown by conducting a complete security assessment.

Present in [5] are Ding Wang et al. Wenting Li and Ping Wang Two-factor authentication strategies have been offered by a number of firms in the current remote sensor industry. However, as a general rule, convention organisers promote the advantages of their strategy, but do not reveal the areas in which their plan falls short of their expectations. The "break fix-break fix" loop in this examination zone is a result of a lack of a level-headed, far-reaching evaluation. Delegate plans are estimated using our assessment technique and the missing evaluation is given to two-consideration plans in current WSNs. This project will assist increase our understanding of current estimating challenges and enhance the logical cycle in our industry..

III. PROPOSED SYSTEM

With the Hub Catch Assault scientific classification of WSN hub catch attacks, we usually expand the model "protection against hub catch assaults" into 10 types. Under our expanded measures set, we do an enormous scope examination of 61 WSN client validation strategies. There are only two of these plans that are safe against hub capture attacks, illustrating the difficulty in creating hub catch assault safe client verification strategies for WSNs in transit. Although our study provides a better understanding of hub capture attacks, we believe our work will aid in the design of WSN client validation strategies that are resistant to hub catch attacks is shown in figure 1.

IV. ARCHITECTURE DIAGRAM

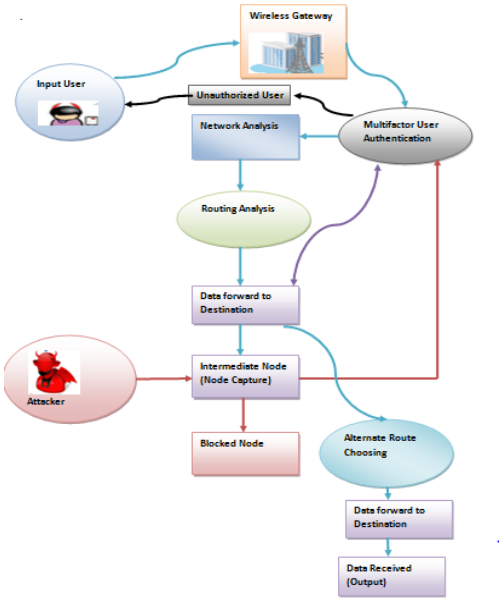

Figure.1. Architecture diagram

V. MODULES

- Network analysis
- Routing Analysis
- Multi factor Authentication
- Node Capture Attacker detection
- Received User

VI. MODULES EXPLANATION

NETWORK ANALYSIS

Take a pre-determined route from the centre of the city. For this walk to be successful, it must be long enough such that all of the peers it visits are able to address a close example from the primary fixed circulation. The framework subtleties and interaction subtleties of the peers you visited may be retrieved. It's become a hub of activity for the company. When sending a solicitation and receiving a response, both the sender and the recipient were involved.

ROUTING ANALYSIS

It's the connections with high force percentage and connection term that are linked to courses. Energy savings are achieved by reducing the number of hub disappointments. A hub disjunct route depending on energy and bounce for information movement will be chosen and the surplus ways will be stored in reserve at that time. In the event that the fundamental decision fails, a need-based approach to maintenance is also provided for determining alternative routes depending on surplus energy in reserve. As a result, throughput is enhanced as a result of the excellent connection quality. Using a higher layer like an organisation layer, information may be efficiently transferred even in a challenging environment. We need to know the location of the distant company in order to be competent in directing. Because of this, we are able to speed up the directing cycle and send shipments more efficiently with a high percentage of bundles delivered. Using a rate, the user may determine how long it will take them to get to their destination. By reducing transmission energy consumption, way selection and support extend the life of the organisation.

It is suited for asset forced situations since it requires just cryptographic hash capacity and elite OR activity. In spite of this, the Cryptographic scheme has certain flaws and is vulnerable to various attacks that were avoided in the suggested alternative structure. HMAC plans include imperfections and are vulnerable to a variety of attacks, including those that take the form of a stolen hub catch. We suggest an enhanced multilayered client authentication that can withstand hub catch attacks as well as other common types of attacks, in order to overcome the security flaws of the two schemes.

Sending out a Request message to all the neighbouring hubs, the source hub is looking for a route at this time. The information stored in certain sensor hubs may be readily accessed by an adversary since they are often given in unattended mode. The framework's security must be maintained once the sensor hub has been hacked. Efforts have been made to devise defences against such an assault, but many others have failed. Hub catch attacks have a logic, and in this section, we summarise that rationale and provide some recommendations on how to prevent them. The ability to identify an attack rather than depending on cryptographic-based techniques. Because they're all disguised up as the same person, no one else can tell how many attackers there are. Even if our attackers modify their transmission power levels to mislead the layout of their actual locations, we can still contain a big number of them. The manner assistance is engaged in the case of a delivery failure to manage the information transfer. Each of the course's hubs is responsible for determining whether or not the connection to the following jump is broken. When the retransmission and affirmation component determines that the connection has been terminated, it sends an RERR package to the source. If there are any further courses available, the hub will check its course reserve. If the parcel header's source course needs to be changed, then this new course will be used to dispatch the package if it is available [16-25].

Sensor hubs may communicate with one another through signals. A remote sensor hub includes equipment for detecting and recording, as well as radio handsets and force segments. As a result of their high speed of preparation, stockpiling capacity, and data exchange, remote sensor networks (WSN) depend heavily on their particular hubs. Multi-jump communication is used to connect with the sensor hubs, who are responsible for developing an appropriate organisational structure. At this point, the information client's local sensors begin acquiring relevant data from their surroundings. When you're closer to the attacker, you have a better chance of seeing it. The location rate jumps to 100% when the satirising hub is within 45-50 feet of the original hub.

VII. CONCLUSION

The most important advancement in the investigation of hub catch attacks against WSN client verification protocols. We begin by defining the opponent model, and then build up a detailed and thorough evaluation, including the effects of hub catch attacks, which are included in this assessment. We then categorise hub catch attacks into 10 unique types based on the attack's goal, the enemy's capabilities, and the flaws that are exploited in the assault. In the next section, we examine weak conventions and compare countermeasures for each kind of attack. In the end, we enlarge our evaluation criteria and direct an enormous scope, such as the estimate of 61 agent client confirmation strategies for WSNs. It is important to note that just two of these plans are resistant to hub catch attacks, demonstrating the difficulty in developing WSN hub catch assault safe client validation plans and the significance of our thorough analysis into hub catch assaults.

REFERENCE

[1] M. Wazid, A. K. Das, V. Odelu, N. Kumar, and W. Susilo, “Secure remote user authenticated key establishment protocol for smart home environment,” IEEE Trans. Depend. Secur. Comput., 2017, doi:10.1109/TDSC.2017.2764083.

[2] S. Kumari and H. Om, “Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines,” Comput. Netw., vol. 104, no. C, pp. 137–154, 2016.

[3] J. Wei, X. Hu, and W. Liu, “An improved authentication scheme for telecare medicine information systems,” Journal of medical systems, vol. 36, no. 6, pp. 3597–3604, 2012.

[4] X. Yang, X. Yi, I. Khalil, Y. Zeng, X. Huang, S. Nepal, X. Yang, and H. Cui, “A lightweight authentication scheme for vehicular ad hoc networks based on msr,” Vehicular Commun., vol. 15, no. 16–27, 2019.

[5] M. Wazid, A. K. Das, M. K. Khan, A. D. Al-Ghaiheb, N. Kumar, and A. Vasilakos, “Design of secure user authenticated key management protocol for generic iot networks,” IEEE Internet of Things J., vol. 5, no. 1, pp. 269–282, 2018.

[6] D. Wang, W. Li, and P. Wang, “Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks,” IEEE Trans. Ind. Inform., vol. 14, no. 9, pp. 4081–4092, 2018.

[7] M. L. Das, “Two-factor user authentication in wireless sensor networks,” IEEE Trans. Wirel. Commun., vol. 8, no. 3, pp. 1086–1090, 2009.

[8] Y. Zhang, Y. Xiang, and X. Huang, “Password authenticated group key exchange: A cross-layer design,” ACM Trans. Int. Tech., vol. 15, no. 4, pp. 24:1–24:20, 2016.

[9] W. Meng, Y. Wang, D. S. Wong, S. Wen, and Y. Xiang, “Touch behavioral user authentication based on web browsing on smartphones,” J Netw. Comput. Appl., vol. 117, pp. 1–9, 2018.

[10] E. Erdem and M. T. Sandıkkaya, "Otpaas—one time password as a service," IEEE Trans. Inform. Foren. Secur., vol. 14, no. 3, pp. 743–756, 2018.
[11] J. Srinivas, A. K. Das, M. Wazid, and N. Kumar, "Anonymous lightweight chaotic map-based authenticated key agreement protocol for industrial internet of things," IEEE Trans. Depend. Secur. Comput., 2018, doi: 10.1109/TDSC.2018.2857811.
[12]S.Kannadhasan, G.Karthikeyan and V.Sethupathi, A Graph Theory Based Energy Efficient Clustering Techniques in Wireless Sensor Networks. Information and Communication Technologies Organized by Noorul Islam University (ICT 2013) Nagercoil on 11-12 April 2013, Published for Conference Proceedings by IEEE Explore Digital Library 978-1-4673-5758-6/13 @2013 IEEE
[13] D. Wang and P. Wang, "Two birds with one stone: Two-factor authentication with security beyond conventional bound," IEEE Trans. Depend. Secur. Comput., vol. 15, no. 4, pp. 708–722, 2018.
[14] D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and approaches for distributed sensor network security," NAI Labs Technical Report #00-010, http://download.nai.com, Tech. Rep., 2000.
[15] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proc. IEEE S&P 2003, pp. 197–213.
[16] Rangaraj, R., Sathish, S., Mansadevi, T. L. D., Supriya, R., Surakasi, R., Aravindh, M., ... & Osman, S. M. (2022). Investigation of weight fraction and alkaline treatment on catechu linnaeus/Hibiscus cannabinus/sansevieria ehrenbergii plant fibers-reinforced epoxy hybrid composites. Advances in Materials Science and Engineering, 2022.
[17] Ganesh, S. S., Kannayeram, G., Karthick, A., & Muhibbullah, M. (2021). A novel context aware joint segmentation and classification framework for glaucoma detection. Computational and Mathematical Methods in Medicine, 2021.
[18] Munimathan, A., Sathish, T., Mohanavel, V., Karthick, A., Madavan, R., Subbiah, R., ... & Rajkumar, S. (2021). Investigation on heat transfer enhancement in microchannel using Al2O3/water nanofluids. International Journal of Photoenergy, 2021.
[19] Aravindh, M., Sathish, S., Ranga Raj, R., Karthick, A., Mohanavel, V., Patil, P. P., ... & Osman, S. M. (2022). A Review on the Effect of Various Chemical Treatments on the Mechanical Properties of Renewable Fiber-Reinforced Composites. Advances in Materials Science and Engineering, 2022.
[20] Hmidet, A., Subramaniam, U., Elavarasan, R. M., Raju, K., Diaz, M., Das, N., ... & Boubaker, O. (2021). Design of efficient off-grid solar photovoltaic water pumping system based on improved fractional open circuit voltage MPPT technique. International Journal of Photoenergy, 2021.
[21] Rajendran, V., Ramasubbu, H., Alagar, K., & Ramalingam, V. K. (2021). Performance analysis of domestic solar air heating system using V-shaped baffles–an experimental study. Proceedings of the institution of mechanical engineers, part E: journal of process mechanical engineering, 235(5), 1705-1717.
[22] Sathish, T., Mohanavel, V., Karthick, A., Arunkumar, M., Ravichandran, M., & Rajkumar, S. (2021). Study on Compaction and machinability of silicon nitride (Si3N4) reinforced copper alloy composite through P/M route. International Journal of Polymer Science, 2021.
[23] Kumar, R. R., Thanigaivel, S., Dey, N., Priya, A. K., Karthick, A., Mohanavel, V., ... & Osman, S. M. (2022). Performance Evaluation of Cyclic Stability and Capacitance of Manganese Oxide Modified Graphene Oxide Nanocomposite for Potential Supercapacitor Applications. Journal of Nanomaterials, 2022.
[24] Sujith, A. V. L. N., Swathi, R., Venkatasubramanian, R., Venu, N., Hemalatha, S., George, T., ... & Osman, S. M. (2022). Integrating nanomaterial and high-performance fuzzy-based machine learning approach for green energy conversion. Journal of Nanomaterials, 2022.
[25] Pazhanimuthu, C., Baranilingesan, I., & Karthick, A. (2021). An improved control algorithm for series hybrid active power filter based on SOGI-PLL under dynamic load conditions. Solid State Communications, 333, 114357.