International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Enhanced Security through Multi-Tier User Authentication in Wireless Sensor Networks

S.V. Achuta Rao , M. Venkata Rao

Abstract: ***Paper Setup must be in A4 size with Margin: Top 0.7", For Smart Home Appliance Devices (SHAD), a Wireless Sensor Network (WSN) utilized for monitoring the condition and controls of SHAD to supervise lighting, warming, security, and investigation. A user confirmation method is required that enables authenticated clients to access SHAD managements for securing SHAD. Providing authentication is a challenging task despite the limited properties of sensor nodes. This proposed Multi-Tier User Authentication Scheme (MTUS) a proficient and security upgraded secret validation with a key acceptance method by utilizing biometrics data as the confirmation factor. Thus, the proposed MTUS method achieves a high-security level by time consumptions, which have 0.454 m sec of improvement of user verification. MTUS comprises of tasks and less time consumptions by existing method of Denial-of-Service(DoS)-Resistant User Authentication (DRUA) systems. Thus, the proposed MTUS method is with Denial-of-Service(DoS)-Resistant User Authentication (DRUA) existing systems. The MTUS proposal increases the demonstration of the system by reducing SHAD traffic, guarding against DRUA assaults, and increasing the battery lifetime. Subsequently, the usefulness and execution of the whole system are improved***.

Keywords: Wireless Sensor Network, User Authentication, Multi-Tier Architecture, Security, Verification.

I. INTRODUCTION

A wireless sensor association contains nodes in considerable numbers to assemble and transmit regular data to a gathering point named Base Station (BS) [1]. These frameworks have particular energy for military applications, characteristics, home robotisation, therapeutic, and a critical number of applications related to the checking of essential establishments. A customer can access to the assembled data either really or remotely. In the first case, a user with a mobile device discusses straightforwardly with the sensor hubs. For security reasons, access to the sensor systems should be controlled. Accordingly, to guard the system against different attacks, we proposed a verification answer for this portable user. We think that confirming remote users in WSNs is a significant security issue because of their unattended and antagonistic organizations. Also, sensor hubs are generally furnished with constrained computing authority, gathering, and correspondence modules.

Consequently, verifying remote users in such asset compelled condition is a test security concern [2] .For WSN application; we offer an equipped user verification method in this paper. This method beats the verification issue and improves the adequacy of WSNs. We propose verification methods called the Multi-Tier User Authentication Scheme (MTUS). The reasons for the scheduled verification mechanism are as per the following:

- ❖ By decreasing system traffic, the system execution increased;
- ❖ Save the battery intensity of the nodes, in this way upgrading the lifetime of the WSN; and
- ❖ Defend the sensor arrange against various kinds of assaults, in this way improving the usefulness and execution of the whole system

The organization of this paper is composed as pursues: Section 2 talks about the user validation issues in existing WSN. In Section 3, we portray our proposed user validation structure. Area 4 gives the security parts of the proposed security for user verification levels. Segment 5 shows the evidence of the noteworthiness of execution correlation with the existing technique. At last, Section 6 gives closing comments in regards to this exploration.

II. LITERATURE REVIEW

Numerous client validation and key understanding method have been proposed in the most recent decade to improve the security of WSNs. In 2006, because of lightweight activities, for example, XOR tasks and single direction hash work, Wong et al. proposed a lightweight solid secret key validation plot for WSNs. Notwithstanding, Das brought up that Wong et al. Conspire is defenseless against the same login character assault, replay assault, and taken verifier assault. Das, at that point, exhibited a two-factor confirmed key foundation plot for WSNs as an improved adaptation of Wong et al. Conspire [3].

A user verification scheme on dependent on the secret user word and cryptographic hash sizes. This ides is powerless against various security assaults, for example, fashioned, replay, and taken verifier assaults. Since a portal and login hub keeps up tables containing enlisted user data, user passwords might be uncovered by any of the sensor hubs, and a user might be obstructed from adjusting their secret code.

Manuscript published on November 30, 2019.
* Correspondence Author
Dr. S.V.Achuta Rao Professor*, St. Martin's Engineering College, Dhulapally, Secunderabad, India - 500100, drsvarao@gmail.com
Dr.M.Venkata Rao, Professor, St. Martin's Engineering College, Dhulapally, Secunderabad, India - 500100, mvrao239@gmail.com

A smart card and secret key based user verification method gives no security to user behavior. It is powerless to disconnect secret key speculating assault, and the smart card has taken the attack, and session key compromise assaults are possible. Sung Jin et al. proposed a brilliant card-based verification convention for remote sensor organize in vehicular correspondence.

The key length characteristic likewise influences the strength utilization at the sensor node; the RSA-1024 calculations expend 4.9 occasions the energy of ECC-160 calculations. Contrasted with ECC-160, an RSA-1024 handshake also consumes 2.7*ms*times the energy in transmitting and accepting information. Correspondence costs for RSA-1024 are higher in light of the more extended key sizes, in this way, making the endorsements bigger also. With RSA-1024 [7], the entire handshake requires the customer to transmit 490 bytes of payload and the server to send 314 *bytes* of payload. With ECC-160, the two gatherings communicate a similar measure of payload information, 138 bytes [4].

User confirmation, on the other hand, and key understanding methods dependent on the idea of IoT proposed. In 2014, Turkanovi'c et al. proposed an energy proficient user validation scheme with high security and low computational cost utilizing the concept of the IoT. Be that as it may, Farash et al. discovered that Turkanovi'c et al.,the scheme has security shortcomings and afterward proposed an improved method. In 2016 [8], Amin et al. guaranteed that Farash et al. the system has some security issues, for example, known session-explicit brief data assault, disconnected secret word speculating attack utilizing a taken smart card, another smart card-issue attack, user impression attack, weakness of the mystery key of the gateway hub, and weakness of user insignificance. Amin et al. [5],at that point, proposed an insignificance safeguarding three-factor validated key trade scheme for IoT-based WSNs [9].

III. WSN ARCHITECTURE: MULTI-TIERED WSN ARCHITECTURE

The conventional design of WSNs consistently accepts that a believed base station is available and liable for gathering information from the sensor hubs and handling question demands from the users. We can see that such engineering only makes sense for exploratory and miniature systems. In any case, a few WSNs are sent in unfriendly and vicious situations, for example, war zones, forests, and seas where it is unthinkable or hard to build up a steady correspondence interface from sensor hubs to the base station that is the reason enormous scale WSNs pursue a two-layered design. In a two-tiered network as delineated in Figure 1, two kinds of nodes are sent, and commitment is separated among those nodes. The entire system is partitioned into clusters; then, each cluster speaks to a particular area in the system. The low skilled nodes perform detecting and transferring data to the Cluster-Head (CH) [10] called Sensor Node (SN) likewise. The SN, which has a higher capacity than different nodes, aggregates the received information and transmits the data to the BS. It expends more power contrasting with the large scale sensor nodes [6].

A. The Multi-tiered WSN architecture benefits are:

- Cluster structure gives the impression of a littler and progressively stable system
- Energy utilization and storage-saving just as the effectiveness of query handling
- Data collection implies that information from gatherings of nodes is totaled before being transmitted; this can enormously decrease use by eliminating repetitive information.
- Improving system lifetime: sensor nodes will spare a lot of intensity since they will be less now and again associated with the correspondence procedure.
- Reduce system traffic and the conflict for the channel
- Security and authenticity should be assured. In any case, the CPUs on the detecting nodes can't deal with an extravagant encryption scheme, so we utilize the gateways node to achieve the cryptographic capacities.

IV. PROPOSED METHOD

For coordinated web WSN, we create a lightweight secured protocol in this paper by utilizing Eclipse Curve Cryptography. For this situation, the encryption and decoding procedure is very verified and lightweight [11]. As this is lightweight, it is exceptionally reasonable for WSN. There are four significant modules user enlistment, server enrollment, sensor node enlistment, and login. In our proposed work, for three-factor validation, we utilize the accompanying verification of user qualification data, client biometric data, and mystery keys. Figure 1 shows the design of the proposed framework.

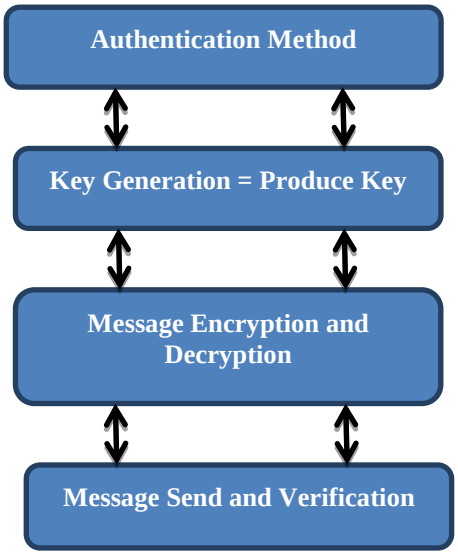

Fig1. Proposed WSN Architecture for Authentication

A. System Setup Phase

This stage is executed by home entryway in a disconnected mode before sending of sensor nodes in an objective field.

- SN produces arbitrarily two secret master keys for all users and all sensor nodes, separately, which are just known to SN [12].
- For every sensor node Sj, SN chooses a unique identity and computes.
- Finally, every sensor node is conveyed in the scientific field in the wake of putting away and its memory in a safe way.

B. Algorithm 1: Registration & Authentication Phase

Begin

User = BS [User $_{ID}$, V]
BS = User [s]
User =SN [User $_{ID}$, V, $T0$, RI]
Sensor Node = BS [User $_{ID}$, y, Time]

If V ≠ V **Then**

BS = Sensor Node [Active]
BS = Sensor Node [Accept, Sender, Time]
Sensor Node = User [Accept, Receiver, Time]

End

C. User Registration Phase

The client enlistment stage starts when a user sends a request message for enrollment to SN over a protected channel. The user enrollment stage for the proposed method. This stage is depicted in figure 2.

a) The user chooses the ideal character and secret key and engravings client biometrics. The client produces a random unknown number and registers. The user, at that point, sends an enlistment request to SN over a protected channel [13].
b) Upon getting the user's enrollment request, SN arbitrarily chooses a one of a kind one-time pen pseudonym
c) After accepting the smart card and save.

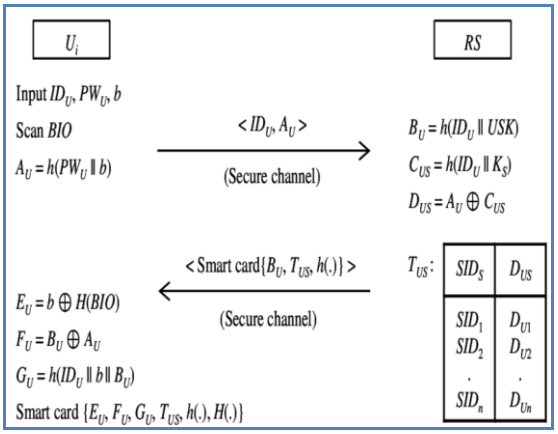

Fig. 2. The user registration phase for the proposed scheme

D. Login Phase

To access the WSN utilizing IDs [14], the login stage is executed when the user needs it. The login and validation stages for the proposed methods. This stage contains the accompanying advances.

- User supplements inputs ID and PW, and engravings client biometrics.
- Computes bio ID and checks whether Bio ID matches with the stored Bi. On the off chance that it matches guarantees that the user has given the right ID, PW, and Bio ID. At that point chooses an irregular number and figures ID
- Finally, the user sends a login request to the gateway over an open channel.

E. Authentication Phase

The validation stage starts when the gateway gets the login demand from the user. For accomplishing standard confirmation and session key understanding, this stage executes in a few steps, as following figure 3.

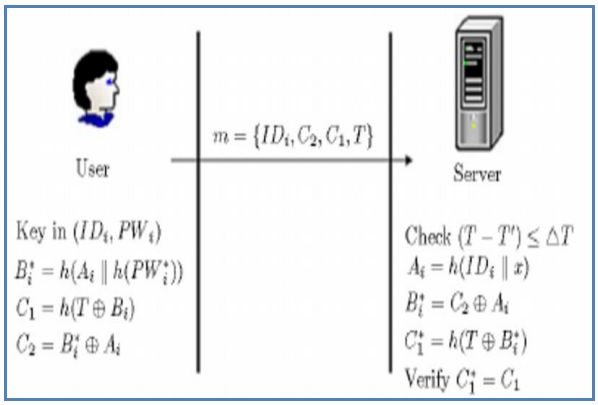

Fig 3. Login and authentication phases for the proposed scheme.

F. Password Change Phase

The secret key change stage starts when the user needs to change the first secret key to another Password new. This stage contains the accompanying figure 4.

- User supplements inputs ID, PW, and another secret key and imprints biometrics into a terminal.
- Computes Bio ID at that point contrasts Bio ID and the stored Bio ID. If this condition isn't fulfilled, it ends this stage. Something else plays out the following step.

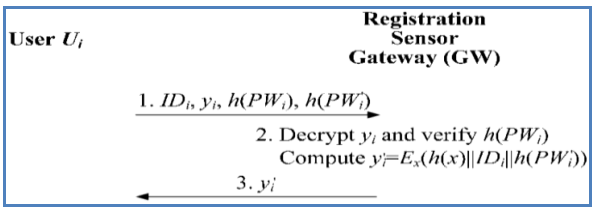

Fig 4. Password change phase for the proposed scheme.

V. RESULT AND DISCUSSION

In this segment, we assess an exhibition like computational expense and security highlights with recently proposed strategies.

The exhibition assessment incorporates Computational coast and security highlights investigation and Communication execution examination. The outline of the computational study shows that our method utilizes just a lightweight hash activity.

A. Communication Cost Analysis

The communication cost of the proposed methods for login and verification stages break down and contrast it with the detailed techniques. For communication cost examination, we assess the communication cost as far as the size of the message in bits and the number of qualities in a note. We accept that the lengths of the character, secret phrase, arbitrary number, and yield of the hash capacity are each 128 bits. We additionally recognize that the lengths of modulo "n" for Rabin cryptosystem utilized in and prime p for ECC used in are each 1024 bits. The cost of user communication, node gateway, and sensor node of the proposed methods and detailed methods are outlined in Table 1, the total communication cost of the proposed method is 1920 bits. The proposed method requires lower communication costs than the above-related methods expect Jung et al. scheme. Even though the proposed method is somewhat less proficient than Jung et al. System regarding communication cost, the distinction (512 bits) isn't huge since the proposed methods have a higher security level.

B. Comparison of Security Features

We analyze the security highlights of the proposed MTUS conspire with other related three-factor validation and essential understanding method of DoS-Resistant User Authentication (DRUA). Tables 1 and 2 show the correlation results. We can see that the first three related method don't ensure all security highlights, in particular, untraceability required for substantial obscurity. The proposed method MTUS and DRUA methods accomplish progressively perfect security highlights and oppose a large portion of attacks. Be that as it may, the DRUA method is costly to actualize and convey in practical applications because of the low execution of Rabin cryptosystem.

Table -I. Comparison of Computational Time of Proposed Scheme

Stages	*Existing DoS-Resistant User Authentication (DRUA)*	*Proposed Method Multi-Tier User Authentication Scheme (MTUS)*
User Action	*3hr.*	*4 hr.*
Server Action	*2 hr.*	*1 hr.*
SNAction	*5 hr.*	*4 hr.*
Login & Verification	*7 hr.*	*5 hr.*
Total Time Computation	*0.691ms.*	*0.454ms.*

Table -II. Comparison of Security Features between Proposed Schemes

User Security Features	*Existing DoS-Resistant User Authentication (DRUA)*	*Proposed Multi-Tier User Authentication Scheme (MTUS)*
Mutual Authentication	*Accept*	*Not Accept*
Secret Key Agreement	*Accept*	*Not Accept*
Password Protection	*Accept*	*Accept*
Dynamic Node Enhancement	*Accept*	*Not Accept*
User Anonymity	*Accept*	*Not Accept*
Attacks	*Accept*	*Accept*

The accompanying figure 5 shows the Performance examination of Time Consumption of DoS-Resistant User Authentication (DRUA) Vs. Multi-Tier User Authentication Scheme (MTUS). What's more, figure 6 showed the different security highlights of DoS-Resistant User Authentication (DRUA) Vs. Multi-Tier User Authentication Scheme (MTUS).

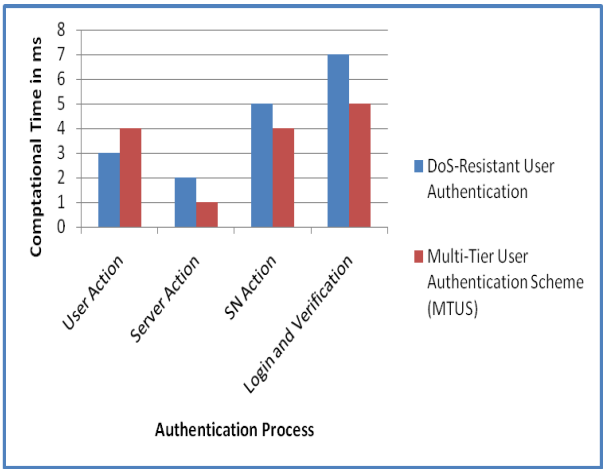

Fig 5. Performance analysis of Time Consumption

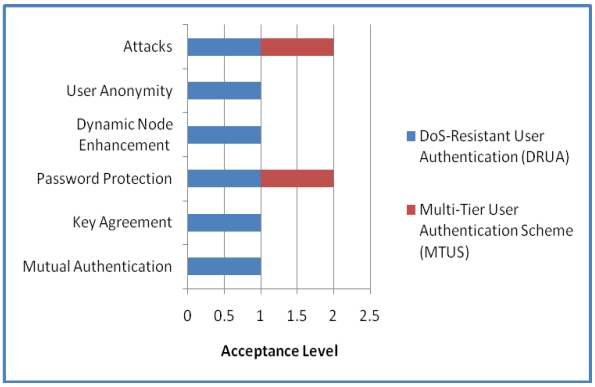

Fig. 6. Performance analysis of Security features

VI. CONCLUSION

The security proposal depends on a secret key retained by the user and a password spared in the user's device. Because of this model, proposed a protected and MTUS confirmation and key understanding idea utilizing the password. Also, we structured our protocol to use fundamental and less time computations. Besides, because of existing DRUA protocols, its computational cost, and energy utilization are regarded to be reasonable for a system resource. Through security investigation, we have demonstrated the proposed MTUS satisfies the user security necessities and opposes different perspectives. We have additionally evaluated the demonstration of the MTUS concerning the time computational and user security overheads. At long last, we have presented a similar examination of the proposed method with DRUA ideas, which legitimize that the proposed MTUS has preferences as far as efficiency and security.

REFERENCE

1. Turkanovi´c, M.; Brumen, B.; Hölbl, M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion. Ad Hoc Netw. 2014, 20, 96–112.
2. Farash, M.S.; Turkanovi´c, M.; Kumari, S.; Hölbl, M. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor networks tailored for the Internet of Things environment. Ad Hoc Netw. 2016, 36, 152–176.
3. Amin, R.; Islam, S.H.; Biswas, G.; Khan, M.K.; Leng, L.; Kumar, N. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. Comput. Netw. 2016, 101, 42–62.
4. Das, M.L. Two-factor user authentication in wireless sensor networks. IEEE Trans. Wirel. Commun. 2009, 8, 1086–1090.
5. Wong, K.H.M.; Zheng, Y.; Cao, J.; Wang, S. A dynamic user authentication scheme for wireless sensor networks. In Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), Taichung, Taiwan, 5–7 June 2006; Volume 1
6. Jung, J.; Moon, J.; Lee, D.;Won, D. Efficient and Security-Enhanced Anonymous Authentication with Key Agreement Scheme in Wireless Sensor Networks. Sensors, 2017, 17, 644.
7. Omar Cheikhrouhou, Anis Koubâa, Manel Boujelben, and Mohamed Abid, "A Lightweight User Authentication Scheme for Wireless Sensor Networks," The ACS/IEEE Workshop: Future Trends on Adhoc and Sensor Networks (FT-ASN 2010), Hammamet, Tunisia, May 16-19, 2010.Adhoc and Sensor Networks (FT-ASN 2010), Hammamet, Tunisia, May 16-19, 2010.
8. Huei-Ru Tseng, Rong-Hong Jan, and Wuu Yang, "A robust user authentication scheme with self-certificates for wireless sensor networks" Security and Communication Networks Security Comm. Networks, (2010).
9. Li, X.; Peng, J.; Niu, J.; Wu, F.; Liao, J.; Choo, K.K.R.: A robust and energy-efficient authentication protocol for the industrial Internet of Things. IEEE Internet Things J. 5(3), 1606–1615 (2018).
10. Sudhakar, S.,Chenthur Pandian, S. Hybrid cluster-based geographical routing protocol to mitigate malicious nodes in mobile ad hoc network, International Journal of Ad Hoc and Ubiquitous Computing , Vol.21, No.4, pp.224,2016.https://doi.org/10.1504/IJAHUC.2016.076358
11. Wu, F.; Xu, L.; Kumari, S.; Li, X.: A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security. J. Ambient Intell. Humanize. Comput. 8(1),101–116 (2017)
12. Karate, A.; Amin, R.; Islam, S.H.; Choo, K.K.R.: Provably secure and lightweight identity-based authenticated data sharing protocol for the cyber-physical cloud environment. IEEE Trans. Cloud Computing.
13. D. Kang, J. Jung, H. Kim, Y. Lee, and D. Won, "Efficient and secure biometric-based user authenticated key agreement scheme with anonymity," Security and Communication Networks, vol. 2018, Article ID 9046064, 14 pages, 2018
14. S.Sudhakar, S.Chenthur Pandian, Investigation of attribute aided data aggregation over dynamic routing in wireless sensor networks,Journal of Engineering Science and Technology, Vol.10, No.11, pp.1465, 2015, 2014
15. O.Althobaiti, R. Mznah, and A. Abdullah, "An efficient biometric authentication protocol for wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 9, no. 5, 2013
16. E.Pagnin and A. Mitrokotsa, "Privacy-preserving biometric authentication: challenges and directions," Security and Communication Networks, vol. 2017, Article ID 7129505, 9 pages, 2017
17. Sudhakar S and Chenthur Pandian, S, A trust and co-operative nodes with affects of malicious attacks and measure the performance degradation on geographic aided routing in mobile Ad hoc network(Article) ",Life Science JournalVolume 10, Issue SUPPL.4, 2013, Pages 158-163

AUTHORS PROFILE

Dr. S V Achuta Rao is working as Professor at St.Martins Engineering College, Secunderabad, India. He has completed his Bachelors and Masters in CS&E from Andhra University and JNT Hyderabad and Ph.D., in CSE from Krishna University, A State Government University, Machilipatnam, Andhra Pradesh, India He is a Life Time Member of ISTE & CSE Society. He is Reviewer and Editorial Board member of reputed International Journals. He has 22 Secunderabad, India. He has 22 years of Teaching experience. His research areas are Empirical Software Engineering, Data Mining, Machine Learning, Soft computing Big Data Analytics and Network Security. He has good number of Patents in Machine Learning & Network Security. He has published more than 60 numbers of Publications in reputed Journals and Conferences. He acted as a Session Chair & Key-note speaker in National and International Conferences.

Dr. M Venkata Rao is working as Professor at St.Martins Engineering College, Secunderabad, India. He completed his Bachelor of Technology from Acharya Nagarjuna University and Master of Technology from JNTU College of Engineering, Hyderabad and Ph.D., in CSE from University of Allahabad. He is a Life Time Member of CSI, IETE & IE (I). He has 22 years of teaching experience. His research areas are Software Engineering, Real-Time Systems, Cloud Computing, Machine Learning, Big Data Analytics and Network Security. He has four Patents. He has published 30 research papers in various Journals and Conferences. He conducted several funded Conferences and workshops.