International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-03, Issue-12, Mar 2018

Most Secured and Flexible Authentication Scheme for Ad Hoc Wireless Sensor Networks

[1]Apurva J. Shastri, [2]Vinayak D. Shastri

[1]PG Student, Department of CSE, M. S. Bidve College of engineering, Latur, Maharashtra, India.

[2]Assistant Professor and Training & Placement Officer in MPGI SOE, Nanded, Maharashtra, India.

Abstract: In Wireless Sensor Network, when user wants to access the data at sensor node at that time user should be authorized. There are many malicious users in network. In previous systems, there are chances of many network attacks like node capture, stolen smart card attack, sensor node spoofing attack, stolen verifier attack, and fails to ensure backward secrecy. To overcome these attacks and to prevent our sensor, sensor data, and Network from malicious users, we proposed a secure, efficient, flexible Authentication Scheme for WSN.

Keywords: Ad hoc wireless sensor network, Smart card, Forward Secrecy, Oracles, Cloud Storage.

I. INTRODUCTION

The authentication in wireless sensor networks is done in two ways:

- A user is authenticated by gateway node before communicating Sensor node.
- A user can directly communicate with sensor node for its authentication.

A sensor node is having some limitations such as-low memory**,** low battery power, low bandwidth, and limited computation ability.

Due to limitations of wireless sensor networks lightweight authentication and key agreement protocols are chosen for wireless sensor networks.

II. RELATED WORK

1. In 2009, M. L. DAS presented a two factor user authentication scheme for WSN, which was mainly intended to obtain strong authentication, session key establishment, and efficiency of the system. The basic idea was user will receive smart card during its registration phase and he can be authenticated with the help of this smart card and his password. But the limitation of this system was experimental results were needed to display feasibility of this scheme and also the counteracts against the denial-of-service and node compromise attacks were not provided.

2. In 2010, [8] proposed an improved two-factor scheme which showed that Das scheme have flaws are vulnerable to attacks like stolen smart card attack and which was resistant to stolen smart card attack as well as other common type of attacks. They depicted security evaluation and efficiency analysis which showed that proposed scheme was more robust and secure than existing system, but the limitations of these scheme was it didn't provided session key agreement and mutual authentication between user and sensor node/GWN. Also the computational overhead of proposed system was insignificantly higher than aforementioned schemes.

3. In 2014, Turkanovicet. Al. proposed a lightweight authentication and key agreement scheme for heterogeneous Ad hoc wireless sensor networks where user can exchange session key with sensor node to which it wants to access very securely by using simple hash and XOR computations. The main aim of paper was providing access of sensor node to remote user without directly contacting the Gateway Node. But the limitation of this paper was the scheme he proposed was prone to attacks like stolen smart card attack, impersonation attack with node capture, sensor node spoofing attack, stolen verifier attack and this scheme was also unsuccessful in providing backward secrecy.

III. SYSTEM DEVELOPMENT

Proposed System with Mathematical Model

User registered to cloud
Select IDi ,PWi Choose random r'I
Select ri Compute.
Compute TIi= h(r'ijjIDi)
TPi= h(rijjPWi) fi = h(TIijj XGW N)
TUreg= IDi,TPiei= TPiŁ fi
Write ri into SCi User Authenticated
CLi= TIi, eI, riCLi = TIi, ei

1)User send data to sensor nodes that time user secure data stored in cloud
Store to S1= fj =h (SIDjjj XGWN).

2) ensor node send data to gateway node, all secure data stored in cloud.
Store to cloud= XGWN,SIDj, XGWN-sj And TIi, XGWN-Uj.

3) session key stored in Cloud.
Store to cloud= SK

 DOI : 10.18231/2454-9150.2018.0063

4) Check session key by session key is maintained or not using cloud stored session.

IV. RESULTS

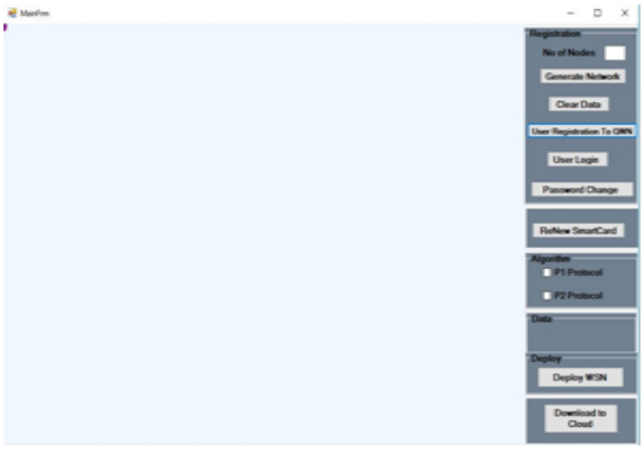

Figure 1: Main Screen

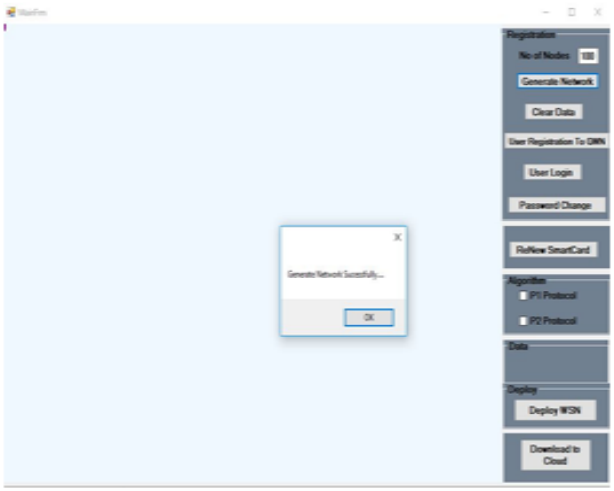

Figure 2: Generate Network

In above figure show the generate network screen. In this screen when you insert number of nodes then click generate network button then you network is generated. And show the message generate network is successfully.

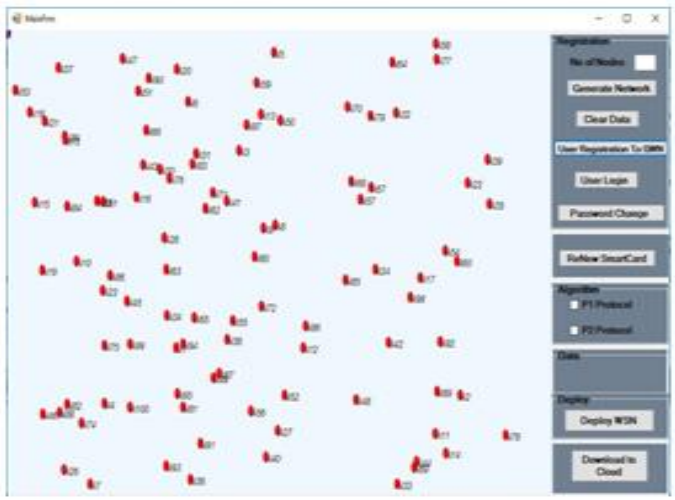

Figure 3: Show Result Generate Network:

In above figure show the result generate network means deploy all node which is inserted in to database randomly.

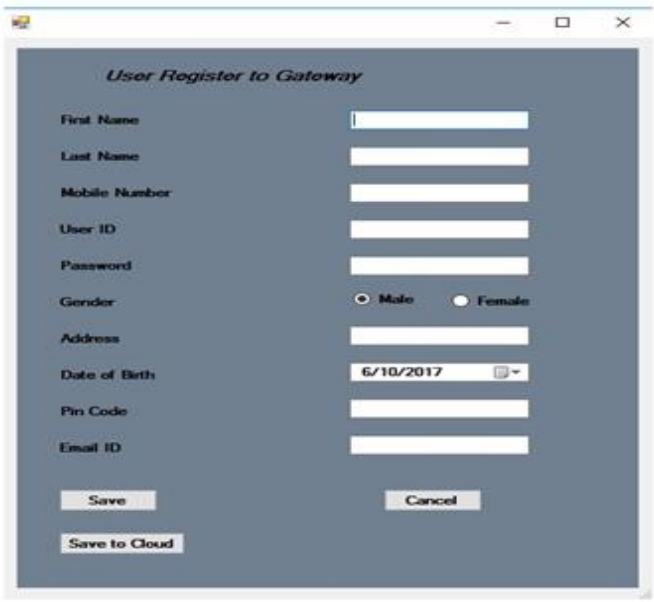

Figure 4 : User Register to Gateway Node

In above figure open a user register form and when you fill all form and click save button that time all fill user information store into database. And user click save to amazon S3 Cloud.

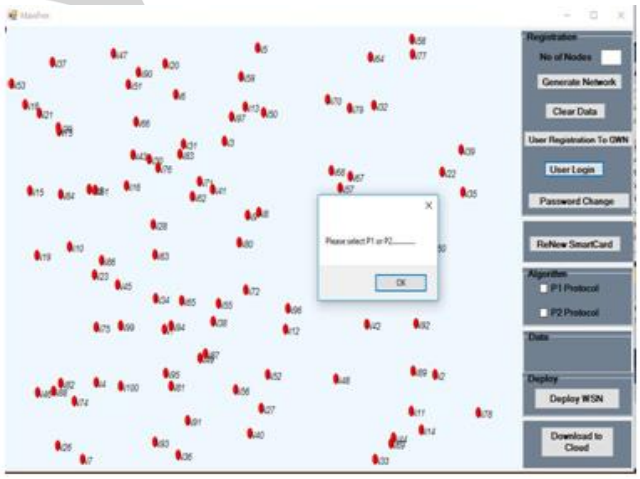

Figure 5 : Select Protocol

In above figure show the message when you click user login without select protocol display message please select P1 or P2 protocol.

Figure 6: Show Result

 DOI : 10.18231/2454-9150.2018.0063

In above figure show the result. When you click to result button then show the compare result P1 and P2.

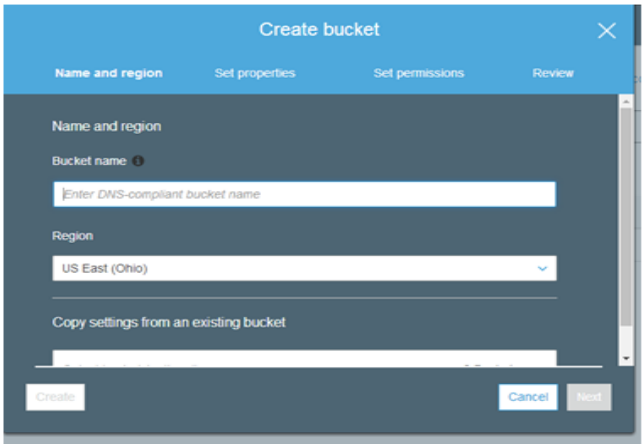

Figure 7: Create Bucket

V. PERFORMANCE ANALYSIS

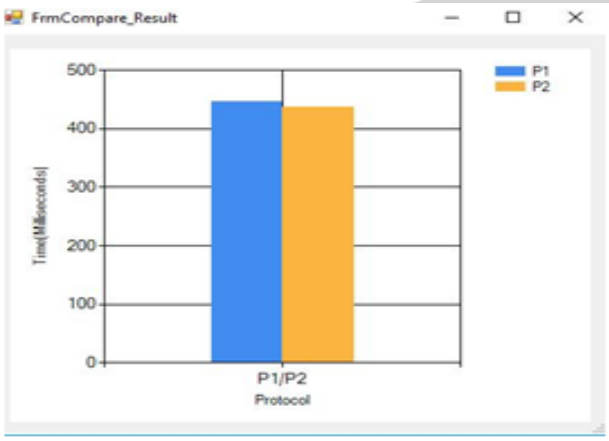

Figure 7: Compare Result

In above figure compare the two protocol P1 and P2. P1 take extra time as compare to P2 protocol. P1 take 450 milliseconds and P2 take 430 milliseconds

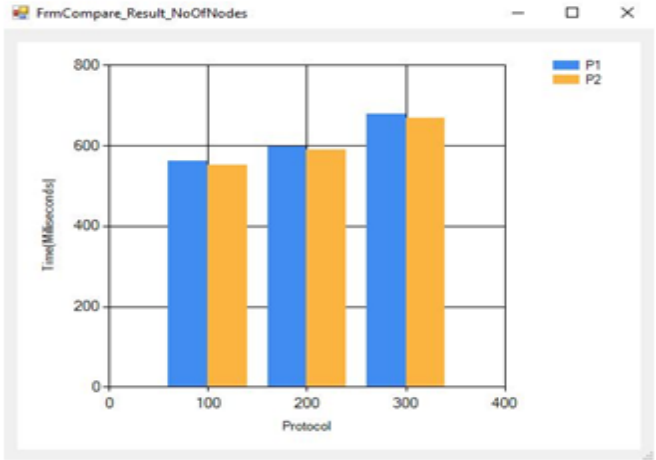

Figure 7: Compare Result by Number of Nodes

In above figure to compare the average result of number of nodes require the how much seconds. In above result take 100 nodes deploy in network P1 take 562 milliseconds and P2 take 552 milliseconds. And second graph bar 200 nodes deploy in network P1 take 599 milliseconds and P2 take 589 milliseconds and last graph bar 300 nodes deploy in network P1 take 678 milliseconds and P2 take 668 milliseconds.

VI. CONCLUSION

Thus, I will implement an appropriate algorithm in such a way that the user can securely access data of the sensors node in network using two authentication schemes. The first overcome the various network attack and second the second scheme is a slightly modified version of the first and it can provide perfect forward secrecy**.** We have also implemented a cloud solution to reduce hardware and storage cost.

REFERENCES

[1] M. Turkanovic, BBrumen, and M. Holbl, "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., vol. 20,pp. 96–112, Sep. 2014.

[2] K. H. M.Wong, Y. Zheng, J. Cao, and S.Wang, "A dynamic user authenticationscheme for wireless sensor networks," in Proc. IEEE Int. Conf.Sens. Netw. Ubiq. Trustworthy Comput., Jun. 2006, vol. 1, pp. 244–251.

[3] H. R. Tseng, R. H. Jan, andW. Yang, "An improved dynamic user authenticationscheme for wireless sensor networks," in Proc. IEEE GlobalTelecommun. Conf., Nov. 2007, pp. 986–990.

[4] M. L. Das, "Two-factor user authentication in wireless sensor networks,"IEEE Trans. Wireless Commun., vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[5] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvementsof two-factor user authentication in wireless sensor networks,"Sensors, vol. 10, pp. 2450–2459, Mar. 2010.

[6] T. H. Chen and W. K. Shih, "A robust mutual authentication protocolfor wireless sensor networks," ETRI J., vol. 32, no. 5, pp. 704–712, Oct.2010.

[7] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factoruser authentication scheme in wireless sensor networks," Ad Hoc Sens.Wireless Netw., vol. 10, no. 4, pp. 361–371, 2010.

[8] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Improved two-factor userauthentication in wireless sensor networks," in Proc. IEEE 6th Int. Conf.Wireless Mobile Comput. Netw. Commun., Oct. 2010, pp. 600–606.

[9] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamicpassword-based user authentication scheme for hierarchical wireless sensornetworks," J. Netw. Comput. Appl., vol. 35, no. 5, pp. 1646–1656, Sep.2012.

[10] K. Xue, C. Ma, P. Hong, and R. Ding, "A temporal-credential-basedmutual authentication and key agreement scheme for wireless sensornetworks," J. Netw. Comput. Appl., vol. 36, no. 1, pp. 316–323, Jan. 2013.

[11] C. T. Li, C. Y. Weng, and C. C. Lee, "An advanced temporal credentialbasedsecurity scheme with mutual authentication and key agreement forwireless sensor networks," Sensors, vol. 13, pp. 9589–9603, Jul. 2013.Elect. Eng., vol. 19, no. 6, pp. 109–116, 2013.

[12] M. Turkanovic and M. Holbl, "An improved dynamic password-baseduser authentication scheme for hierarchical wireless sensor networks,"Electron.Elect. Eng., vol. 19, no. 6, pp. 109–116, 2013.

 DOI : 10.18231/2454-9150.2018.0063