International Journal of Research in Engineering, Science and Management
Volume-1, Issue-12, December-2018
www.ijresm.com | ISSN (Online): 2581-5792

Improvements of "Authentication Protocols in Various Wireless Sensor Networks"

B. Bhavya Sree[1], Latha Manju[2]
[1]*Student, Department of ECE, Saveetha School of Engineering, Chennai, India*
[2]*Professor, Department of ECE, Saveetha School of Engineering, Chennai, India*

***Abstract*: Wireless sensor networks is a combination of different types of sensors for monitoring and noticing the environmental changes and accessing all the collected data at one point. WNSs organize environmental changes like sound, temperature, wind, humidity etc.., Due to its extensive applications wireless sensor networks are used in military applications such as monitoring of battle field, environmental monitoring, and health care monitoring and used in many other applications. As WSN's are involved in highly confidential fields the security of the information collected should be maintained highly confidential. So, authentication plays a key role in wireless sensor networks.in the recent years as the percentage of unethical hacking increased, so security improvements should be developed very rapidly to safeguard the information from hackers and attackers.in this paper we show the applications of authentication in wireless sensor networks and its advancements in the recent years. This paper clearly explains what is authentication and its recent trends in wireless sensor networks.**

***Keywords*: Wireless sensor networks, authentication, attackers**

1. Introduction

Authentication is simply said as a key to open the door of the network which store information. Authentication protocols helps the users to protect the information from attackers and un accessed users of the site. There are various types of authentication protocols based on the improvement in the security techniques. Here, is the list of different types of authentications:

- Single factor authentication
- Two factor authentication
- Multi factor authentication

A. Single factor authentication

Single factor authentication is a security key to access the system or a website. It is like one way to enter into the website or a system. Security wise single factor authentication is not much efficient than the two factor authentication [1]. The only way to develop security is to build a strong password by the user in such a way that no one access. Fig. 1, represents the single factor authentication; it clearly explains that the user identity is verified by a single password. The security is very less in single factor authentication. A good example of two factor authentication is using of ATM card ward withdrawing money. [4] which involves to steps one is the general password which is already known to the user and the other is one time password that get to the user ,and that one time password is verified for only once [5].

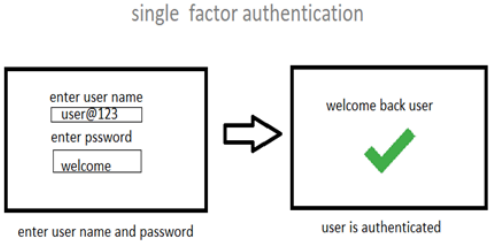

Fig. 1. Single factor authentication

B. Two factor authentication

Two factor authentication is also called as two step verification protocol.it involves two phases first is login phase and the other is verification phase. In two factor authentication the user is provided with two factors to access the system or network [2]. Two factor authentication provides the user better security than the single factor authentication.in single factor authentication the user is provided only with the single step password but where as in two factor authentication the user has two factors to be checked to login in to the site one is as usual the password or any security code and the other is the biometric factor like finger print, face identification and voice recognition etc.., [3]

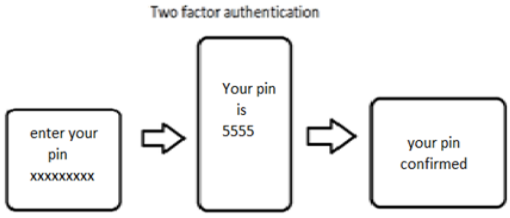

Fig. 2. Two factor authentication

C. Multi factor authentication

In multi factor authentication multiple authentication factors are used to improve security compared to two factor authentication. The two factor authentication is the subset of multifactor authentication. In this the gets access only after the submission of two or more evidences. Figure (1.3) represents the multi factor authentication.

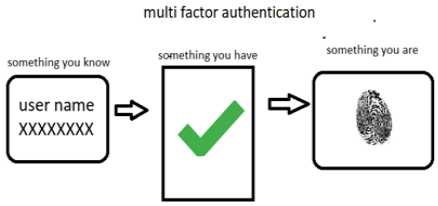

Fig. 3. Multifactor authentication

All these three types of authentication are classified based on the security levels. These are used in different fields of wireless sensor networks. In this paper let us see the applications of authentication protocols in various fields such as: wireless medical sensor networks, authentication protocol in IOT applications, smart card based authentication etc.., and the need of the authentication in that fields.

2. Authentication in various fields

A. Authentication protocol in health care applications

Introduction:

In the recent advancement technology every hospital are organized with wireless medical sensor networks. A wireless sensor network functions in such a way that it will not affect the comfort zone of a patient. These medical sensor networks are particularly aid for continuous monitoring of patient health condition and reporting the details for the user. So the security involved should be high because the data should be protected from unauthorized users. [6]

B. Building of network

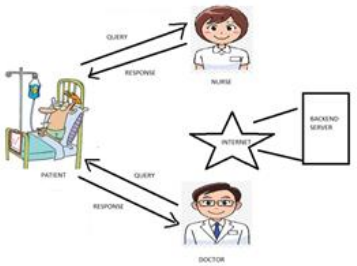

Fig. 4. Health care architecture for patient monitoring

When a patient is admitted in a hospital, the patient is issued with a medical sensor device. This device sense the patient parameters such as blood pressure sugar levels pulse heart beat rate and other body changes, and all these parameters are directly transmitted to the device of the authorized doctors who continuously monitor the patient. It is also possible to send the questions to the patients and the low level staff using this network. Fig. 4, represents the total architecture of the device. The network mainly consists of two nodes namely gateway node and medical sensor node, the user is given by a strong password and username to access the data safely and securely.

C. Related works done on improving the authentication problems

Malasri et al proposed a secured authentication scheme for wireless medical sensor networks [7] the proposed scheme of Malasri et al namely consists of

- Two tier architecture is designed for patient data authentication
- A secure key exchange protocol
- A symmetric encryption /decryption algorithm confidentiality to the data stored

In this scheme the patient identity is verified by his/her fingerprints due to this wrong entry of data is eliminated and this security provides high security to the patients without affecting their comfort zone. However, this scheme does not support strong professional authentication. Hu et al designed a hardware and software based real time cardiac patient health care monitoring system. This network is named as tele cardiology sensor network.it is designed in US health care society and first time implemented in a large nursing home for monitoring elderly patients [8].in this network the ECG signals of patient are collected automatically and transmitted to a wireless channel information is send to an ECG server for further analysis. A block cipher algorithm is used for securing ECG data transmission and for protecting patient privacy. The main drawback of the scheme is the strong user authentication is not addressed effectively. Very recently le et al suggested a mutual authentication for accessing patients data their construction mainly consists of three layers[9] (1)sensor network layer (2)coordination network layer(3)data accessing layer although le et als protocol facilitates security against unauthorized attacks, but their scheme is susceptible to information leakage attacks which leads to the patients privacy. Due to this the patient's vital signs are exposed to illegal users which is not applicable for real time health care applications. In 2009 dass has proposed two factor user authentication protocol for wireless sensor networks [10]. This protocol is safe against replay attack, password guessing attack, stolen verifier, node compromise attack, user impersonation attack, insider attack etc. Later this protocol is susceptible to the gateway bypass attack, user impersonation attack etc. This protocol does not provide confidentiality in the message storage and delivery [11]. Consequently, due to its limitations this scheme is not applicable to health care applications [12]. In [13], Kumar –lee shown some authentication protocols but this scheme has some limitations but the implementation of these protocols costs very high so these protocols are not suitable for such wireless applications

Security requirements:

- Strong user authentication
- Mutual authentication
- Confidentiality
- Session key establishment
- Data freshness
- Secure against popular attacks
- Patient security

Like this the authentication protocols are used in wide range in wireless sensor networks.

Table 1
Literature survey

Basic concept used in authentication	Usability	Efficiency	Security and robustness	Privacy	Adaptability to mcc environment
Using different authentication factors such as ID/Password, IMEI, IMSI, and voice recognition	Very low	High	Fair	Good	Moderate
Message digest based authentication	Low	Low	Very good	Very good	Moderate
Authentication based on user handwriting as a biometric factor	Low	Moderate	Poor	Fair	Low
Authentication using zero knowledge authentication ,digital signature and fuzzy vault	Moderate	Low	Good	Fair	Low
Protecting user password using zero knowledge proof technique	High	High	Good	Fair	Very low
Trust cube authentication	Moderate	Moderate	Poor	Poor	Very low
Fingerprint authentication as an user authentication factor for user authentication	High	Moderate	Poor	Poor	Low
Authentication based on graphical password and biometrics such as voice or face or used together	Very low	Low	Good	Poor	Low

3. Authentication in IoT applications

Wireless sensor networks became more popular in internet of things. In today's world IOT rule the whole world, so security development is focused in this applications .to go in detail with the authentication schemes used in this IOT applications refer [14], and for other applications of authentication refer [15], [16].

4. Literature survey

This survey shows the level of usability, security, robustness and privacy for different types of authentication approaches used in wireless sensor networks, here this table discusses the various security parameters chosen for security development.

5. Future improvement

There is no end for the authentication techniques, as the days passing the wireless sensor networks demands new protocols for security strength and for accessibility. Now a day's mostly research works are carried out on two factor authentication in order to eliminate bypass attacks and to increase the efficiency of the protocols. As we see the tabular column above it reveals that no authentication protocol does not give high usability, efficiency, security and robustness and privacy. If one parameter supports high the other supports drastically low. So, the future improvement will be on this that is generating of authentication protocol scheme which has high security and privacy, efficiency and accessibility.

6. Conclusion

We enclose this paper with the survey details conducted on various security parameters used in authentication and the different types of authentication protocols used in wireless sensor networks. This paper clearly explains the need of authentication in wireless sensor networks. The future improvement on this paper will be on the algorithms used in authentication techniques in various applications.

References

[1] Bigler, Mark. "Single Sign On, Internal Auditor December 2004, 30-34.
[2] Buss, Dale:Two Factor .Too Tough "Security Industries News" June 6 2005 :16-20.
[3] Cryptanalysis Of Two Factor User Authentication In Wireless Sensor Network –Zuowen Tan Advances In Informatics Science And Service Volume 3 Number 4 May 2011.
[4] Pradeep Kumar ,Mangal Sain And Hoon Jae Lee Feb13-16,2011 Icact2011
[5] Ad Hoc and Sensor Wireless Networks, Vol. 10, pp. 361-371, Daojing He,Sammy Chan Jiajun Be
[6] Sensors, www.Mdpi.Com/Journal/Sensors-Sensors 2012,12,1625-1624
[7] Malasri, K.; Wang, L. Design and Implementation of A Secure Wireless Mote-Based Medical Sensor network. Sensors 2009, 9, 6273–6297.
[8] Hu, F.; Jiang, M.; Wagner, M.; Dong, D.C. Privacy-Preserving Telecardiology Sensor Networks:Toward A Low-Cost Portable Wireless Hardware/Software Codesign. Ieee Trans. Inf. Technol.Biomed. 2007, 11, 619–627.
[9] Huang, Y.M.; Hsieh, M.Y.; Chao, H.C.; Hung, S.H.; Park, J.H. Pervasive, Secure Access to A Hierarchical Sensor-Based Healthcare Monitoring Architecture in Wireless Heterogeneous Networks. IEEE J. Sel. Areas Commun. 2009, 27, 400–411.
[10] Das, M.L. Two-Factor User Authentication in Wireless Sensor Networks. Ieee Trans. Wirel.Commun. 2009, 8, 1086–1090.
[11] Khan, M.K.; Alghathbar, K. Cryptanalysis and Security Improvement of 'Two-Factor Userauthentication In Wireless Sensor Networks'. Sensors 2010, 10, 2450–2459.
[12] He, D.; Gao, Y.; Chan, S.; Chen, C.; Bu, J. An Enhanced Two-Factor User Authentication Scheme Inwireless Sensor Networks. Ad Hoc Sens. Wirel. Netw. 2010, 10, 1–11.
[13] Kumar, P.; Lee, H.J. Cryptanalysis On Two User Authentication Protocols Using Smart Card or wireless Sensor Networks. In Proceedings of the IEEE Wireless Advanced (Wiad), London, Uk,20–22 June 2011; Pp. 241–245.
[14] A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor Networks in Distributed IoT Applications, Pawani Poramgage Pardeep Kumar.
[15] Keerti Sreevastava, "A Hash Based Mutual RFID Tag Authentication Protocol in Telecare Medicine Information System."
[16] An Improved Smart Card Authentication Scheme for Session Initiation Protocaol-Seru Kumara, Shehzad Ashraf Chaudary Xiang Li 21 August 2015.
[17] Wong, K.H.M.; Zheng, Y.; Cao, J.; Wang, S. A Dynamic User Authentication Scheme Forwireless Sensor Networks. In Proceedings of the IEEE International Conference On Sensor networks, Ubiquitous, And Trustworthy Computing (Sutc'06), Taichung, Taiwan, 5–7 June 2006.