International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

Server Sensor and Remote Unit Authentication by Smart card

Chittaranjan Chirom
M.E. Anna University, Coimbatore

Abstract **- This project aims to provide mutual authentication of remote unit and remote server side. It uses cryptanalysis process of two user authentication protocols i.e remote unit which is represented by microcontroller and remote server which is represented by personal computer. It consists of registration, login, verification phase in remote server side and login and verification phase for remote unit side. In the registration phase, it explaines how the user password is encrypted and stored in the smart card .In the login phase, it explaines how request message send to remote server and use the response message from remote server for authenticating user .In the verification phase, it explaines how request message handle by the remote server. This project provides more secure format in providing mutual authentication of remote unit and remote server side. All this are done by dot net program in server part and embedded-c program in remote unit part. The efficient ID-based remote user authentication schemes with smart card provides more secure mutual authentication between remote server and remote unit. The efficient ID-based remote user authentication schemes with smart card using only secure one-way hash function. In addition, our schemes provide better trade off among efficiency, flexibility and security than the schemes previously described.**

Keywords **- Wireless Sensor Networks, Registration Phase, Login Phase, Verification Phase.**

I. INTRODUCTION

In recent years, low power sensor nodes have emerged with wireless communication. These wireless sensor networks (WSNs) have accomplished a significant attention due to its wide range of applications in military as well as civilian operations (e.g., military applications, environmental monitoring, healthcare applications, home applications, structural monitoring and numerous commercial applications) . Sensor nodes (e.g., MicaZ and Telos) are the smallest unit of network that has limited memory, low band width, low computation and low power. These wireless sensor networks are deployed to collect the environment data over a geographical area, and later the collected data will send to the user either upon event detection manner or for continuous environment monitoring. However, due to the wireless nature of sensor node it may possible that a user can access sensor data directly without involving the gateway. Smart Card Reader is designed to Read, Write and Authenticate contact cards. It supports various secure cards and Memory cards of several manufacturers like Philips, Siemens, and Atmel etc. So far few user authentication protocols have been proposed for resource constraint wireless sensor network, and each scheme has its own advantages and disadvantages. In 2009, M.L. Das has proposed two-factor user authentication protocol for wireless sensor networks. Das's claimed that his protocol is safe against many attacks (i.e., replay attack, password-guessing attack, user impersonation attack, node compromise attack, and stolen-verifier attack). Later, Nyang and Lee identified that Das's scheme is vulnerable to an offline password-guessing attack by insider, node compromise attack and does not care about other security services, i.e., encryption and authenticity verification of query response. Thus, Nyang and Lee proposed a improvement of Das's two-factor user authentication protocol in WSNs, which overcome the Das's scheme security flaws with some additional security services such as, confidentiality and authenticity of user's query response. In 2010, He et al.'s have shown that Das's protocol is susceptible to insider attack, impersonation attacks and also found design weakness (i.e., about real identity of user).

Later, they proposed an enhanced two-factor user authentication scheme for WSN that ease of user anonymity, safe against insider attack and allow users to change their password. In the same year, Khan and Alghathbar pointed out that Das's scheme is still not secure and cannot resist to many other security attacks, such as, gateway-node bypass attack, does not provide mutual authentication between the gateway and the sensor nodes, vulnerable to insider attack, and user cannot change or update their password, whenever needed. Furthermore, Khan and Alghathbar improved Das's protocol, which provides protection against insider attack, gateway bypass attack and introduced password change phase for users. Unfortunately, this project finds: (1) He et al.'s scheme is susceptible to information leakage attack and cannot preserve user anonymity, no mutual authentication between the user and the sensor, and no session key is establish after user authentication phase between the user and the sensor node; (2) Khan-Alghathbar scheme does not provide mutual authentication between the user and the sensor node, no confidentiality to air messages, and does not establish session key between the user and the sensor node at the end of authentication phase.

II. OBJECTIVE

Cryptography-based security is to protect information resources by making unauthorized acquisition of the information or tampering with the information more costly than the potential value that might be gained. The user authentication mechanism is important part of the Network security, our scheme aims to protect unauthorized access of a network system.

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

III. Existing System

The existing system used cryptanalysis of two user authentication protocols using smart card for wireless sensor networks. This scheme is divided into three phases, namely, registration phase, login phase and verification phase. In the registration phase, each user has given user id and the user password was encrypted and stored in the smart card. In the login phase, it explains how request message send to Remote Server and use the response message from Remote Server for authenticating user. In the verification phase, it explains how request message handle by the Remote Server. In this scheme, registration, login and verification phase was completed in the Remote Server side, where in the Remote Unit side we completed login and verification phase. This scheme provides more secure mutual authentication between Remote Server and Remote Unit. It uses cryptanalysis process of two authentication protocols i.e microcontroller for remote unit side and personal computer for remote server side. It uses dotnet program for remote server side for registration, login and verification phase and embedded c-program for remote unit side for login and verification phase.

IV. Proposed System

In 2009, M. L. Das has proposed a two-factor user authentication scheme for wireless sensor networks, where each user proves his/her legitimacy using password and smart card. Later, in 2010, He et al.'s demonstrated that M. L. Das protocol suffers from insider attack, impersonation attack and users cannot change their password. Then they proposed enhanced two-factor protocol that copes to the Das's protocol weaknesses. In the same year, Khan-Alghathbar pointed out that Das's protocol is suffered from gateway-bypass attack, and no mutual authentication between the sensor node and the gateway. Then Khan-Alghathbar proposed security improvement on Das's scheme.

In this project, we proposed that: (1) He et al.'s scheme is susceptible to information leakage attack, and cannot preserve user anonymity, no mutual authentication between the sensor and the user, and does not establish the session key between the user and the sensor node; (2) Khan- Alghathbar scheme does not provide mutual authentication between the sensor and the user, and does not establish the session key between the user and the sensor node, and no confidentiality to their air messages.

V. Registration Phase

Step1: Insert the smartcard and enter username and password. Step2: Check whether username already exists in the server. Step3: Generate user's random number (b) and hash of random number (b) and user password (PWk) in Remote Server (RS). Step4: Compute secret number (Vk), (Hk) and (Nk) in RS. Step5: Store Vk, Hk, Nk and b in the smart card and RS.

The below flowchart explains the Inserting a Smart Card, Registering or Logging in of new user or existing user and securing the secret keys.

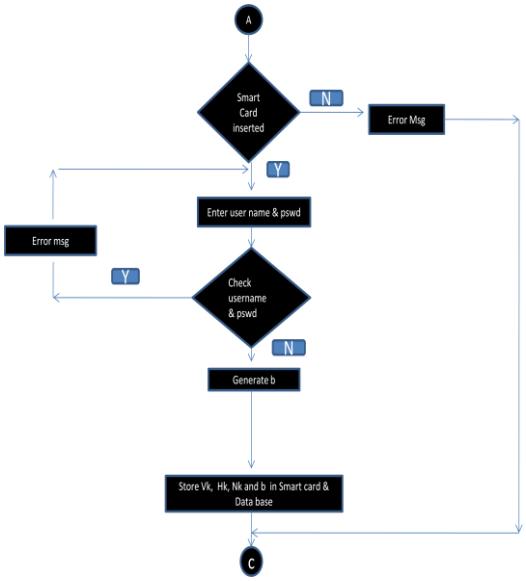
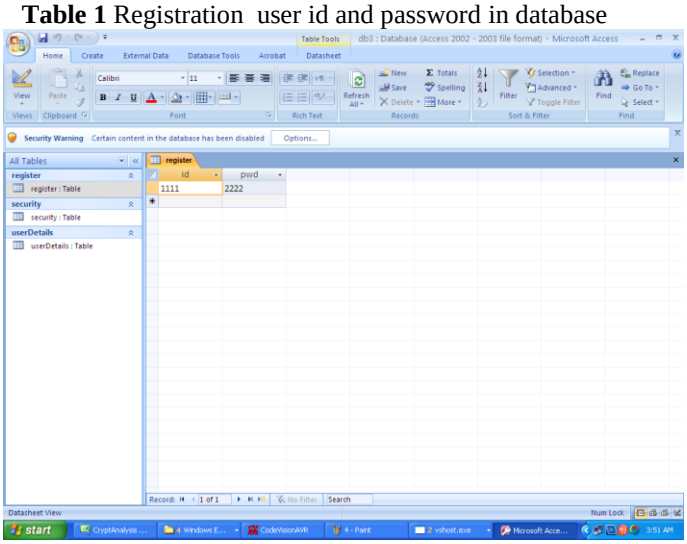


Table 1 Registration user id and password in database



VI. Login Phase

Step1: Insert the smartcard and enter username and password in Remote Unit (RU).

Step2: Compute Tk = Vk ⊕ h (IDk || h (b ⊕ PWk) and HK* = h (Tk).

Step3: Verify Hk* = Hk.

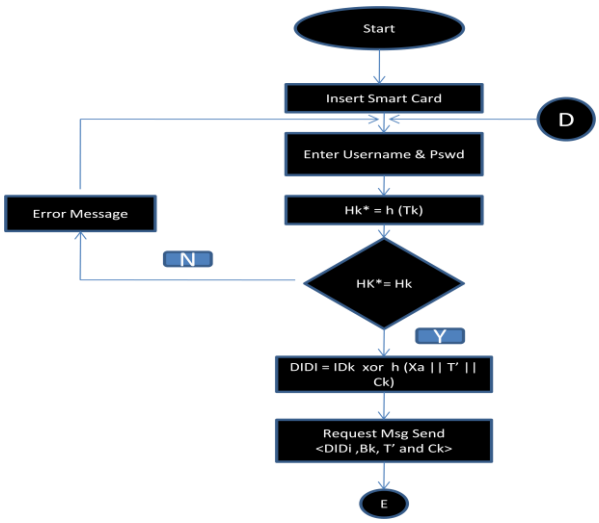
Step4: if the above expression is true then continue the following steps if not terminate the login request.

Step5: Compute DIDk = IDk ⊕ h (Xa || T' || Ck)

Step6: Compute Bk = h (Nk || Xa || T') and then sends login message <DIDk, Bk, T' and Ck).

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

The below flowchart explains the function of Remote Unit side.



VII. Verification Phase

Step1: Receives the request message from RU at timestamp T'.

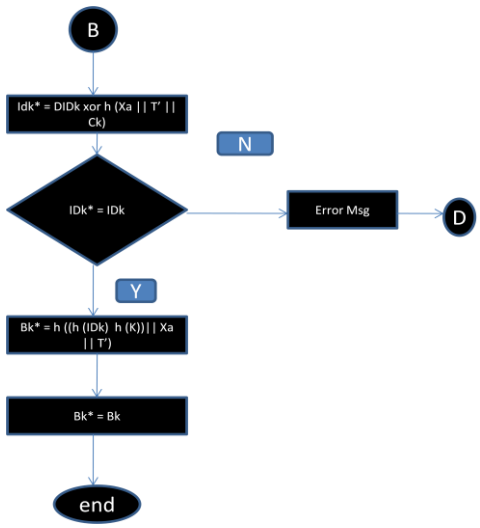
Step2: RS checks for Transmission Delay.

Step3: Then RS Computes IDk* = DIDk ⊕h (Xa || T' || Ck) .

Step4: RS checks whether IDk* is equal to IDk which is received from RU.

Step5: RS computes Bk* = h ((h (IDk) ⊕ h (K))|| Xa || T') and checks Bk* = Bk

The below flowchart it explains how Remote Server handle the request message from Remote Unit.



VIII. Block Diagram

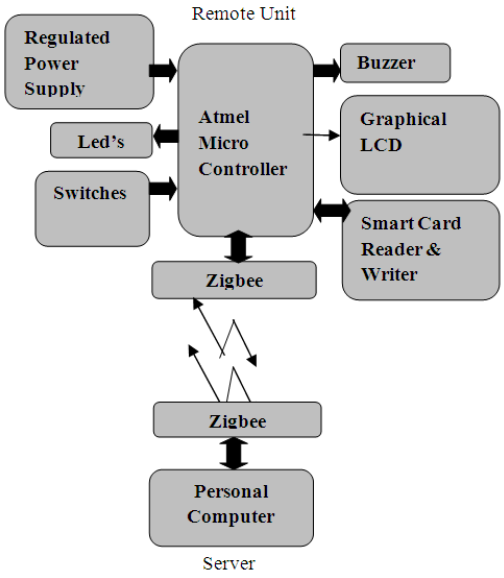


Table 2 Security Table

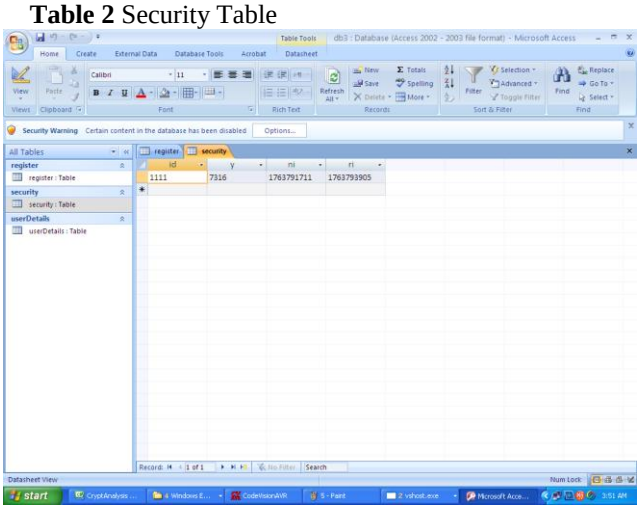
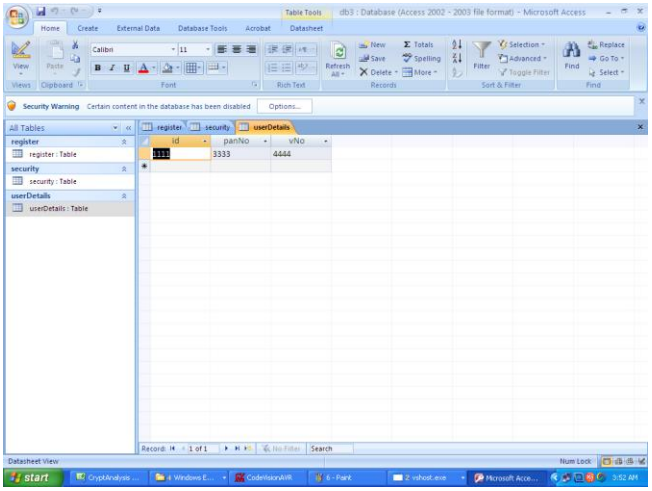


Table 3 User details is stored in database



International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

IX. Input Design

Input design consists of registration phase, login phase and verification phase in remote server side. The Registration Phase consists of Inserting a Smart Card, Registering or Logging in of new user or existing user and securing the secret keys. The Login Phase consists of inserting a Smart Card, Logging in of existing user, get authentication from RS and give authentication to the user. The Verification Phase consists of verifying the request message sent by RU. In remote unit side it input Id and password in microcontroller LCD.When we debug cryptanalysis program of dot net, we obtain following figures in order.

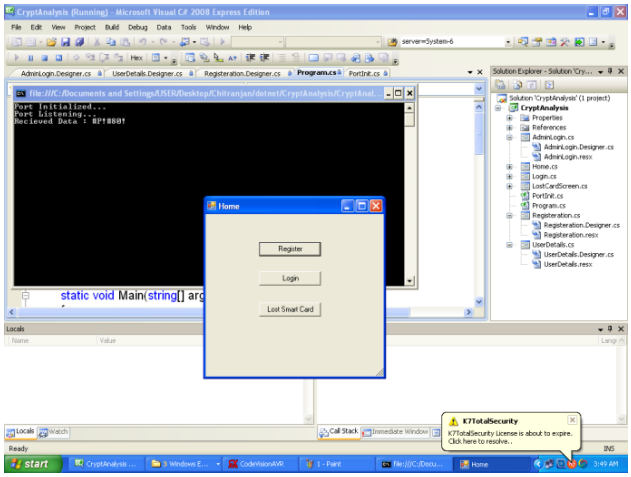


Fig.1. Port Initialization Diagram

On clicking at the register in previous diagram,we get below diagram

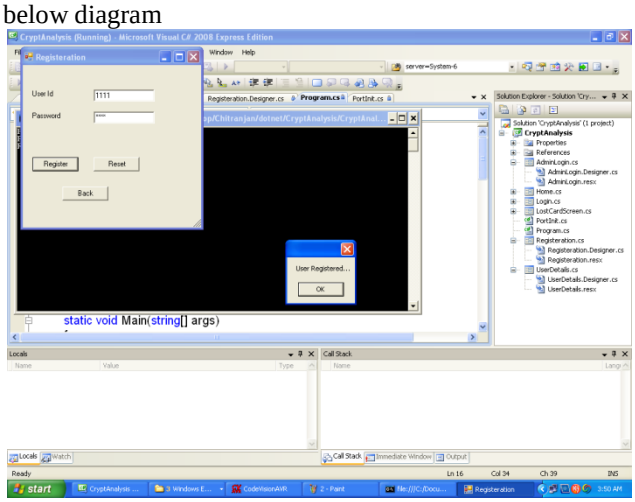


Fig.2. User Registration Diagram

On clicking at login, we get below diagram

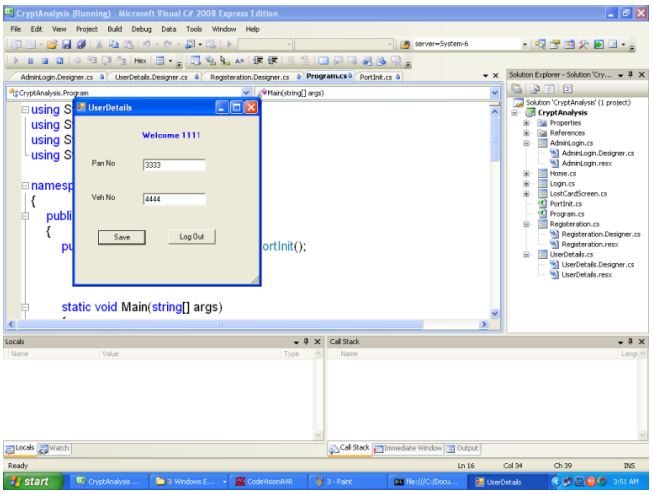


Fig.3. Login Diagram

Fig.4. Input Id and password in microcontroller LCD

X. Output Design

Here it display the Secret key(y), hash function of secret key Ri= h(y), and Ni.

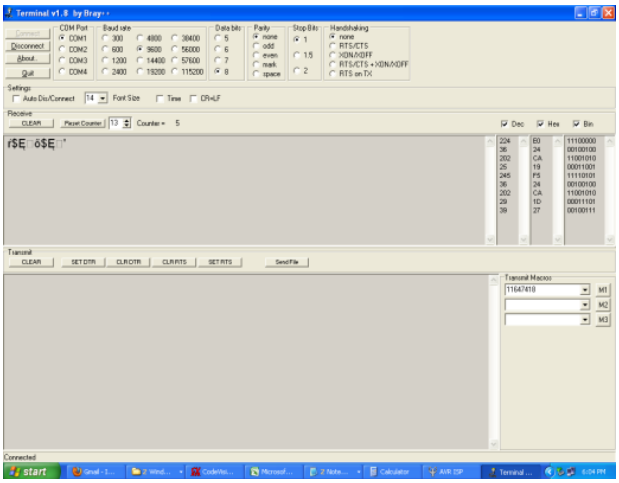


Fig.5. Output for Ni

In login Phase it will compute Pi = Ni ⊕ PWi, DIDi= h (y | Pi | T)

International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 6, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209

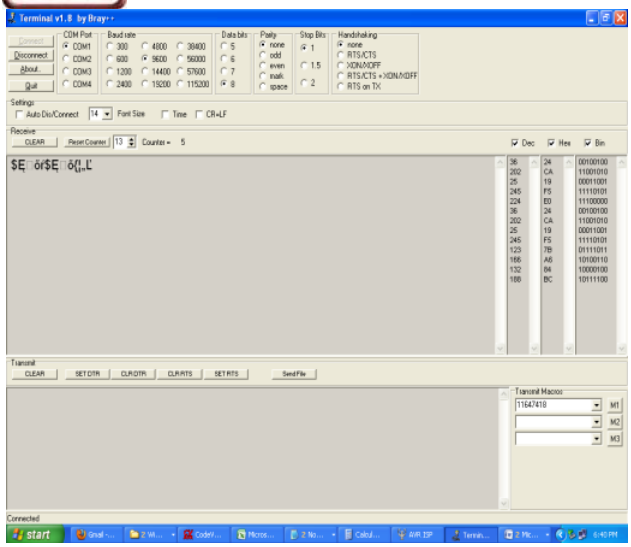


Fig.6. Output for Login Phase (Request message send)

In Login phase after received request message from RS

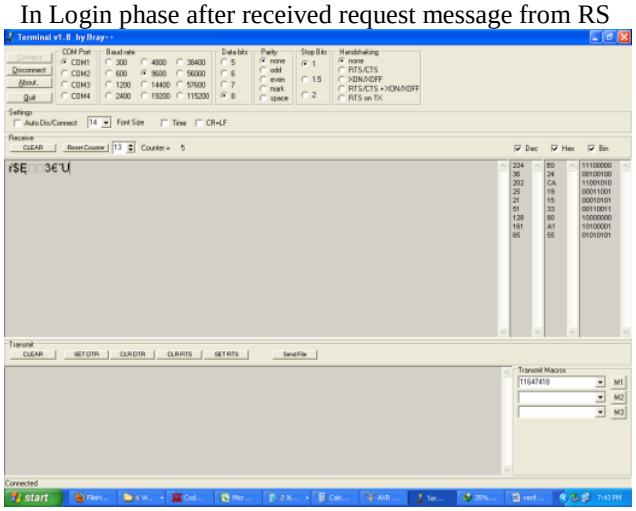


Fig.7. Output for Login phase (Request message Received)

After receiving the request message from RU this phase will compute Ei = h(y ⊕ P | T") and verify.

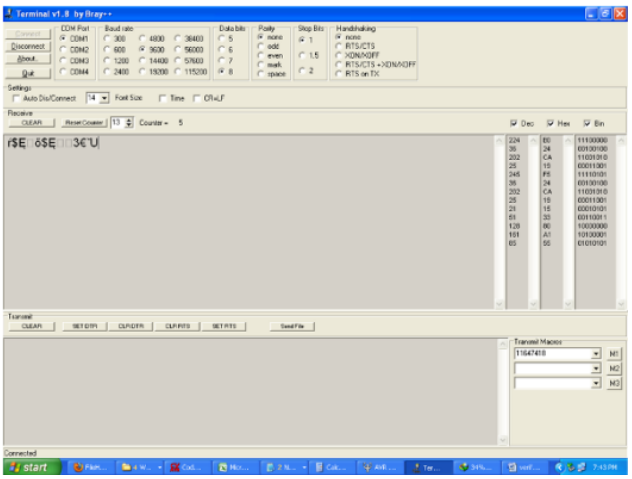


Fig.8. Output for Verification phase

Fig.9. Displaying pan and vehicle number in LCD

Table 4 Notations and descriptions

Notations	Description
IDk	User Identity
PWk	User's password
GW	Gateway node
Sn	Sensor node
B	User's random number
J and xa	High entropy gateway secrets (512 bits
K	Symmetric key of gateway
h(.)	One-way hash function (i.e., SHA-1)
⊕	Bitwise XOR operation
||	Bitwise concatenation operation

XI. RESULT

The efficient ID-based remote user authentication schemes with smart card provides more secure mutual authentication between remote server and remote unit. The efficient ID-based remote user authentication schemes with smart card using only secure one-way hash function. In addition, our schemes provide better trade off among efficiency, flexibility and security than the schemes previously described.

XII. CONCLUSION AND FUTURE WORK

Due to the wireless communication nature of involve entities (i.e., gateway node, and sensor nodes), a user authentication protocol for WSN should facilitates with some specific security services, for example, user anonymity, confidentiality, secure session key establishment, and mutual authentication between the sensor node and the user. This project analyzed the recently proposed two factor user authentication schemes. In He et al.'s scheme, we have found that their scheme is not suitable for real-time wireless sensor networks, because their scheme suffers from information leakage attack, does not take care for user privacy, does not provides mutual authentication between the sensor node and the user, and not able to establish session key after the authentication phase.

Furthermore, we are going to analyze Khan and Alghathbar scheme, which does not does not provides mutual authentication between the sensor node and the user, does not support confidentiality to their air messages, and not able to establish session key after the authentication phase. Also, we are going to implement a password change phase.

REFERENCES

[1] Pardeep Kumar and Hoon-Jae Lee,(2011), "Cryptanalysis on two user authentication protocols using smart card for wireless sensor networks", IEEE, pp. 4577-0109.
[2] Akyildiz I.F., Su W., Sankarasubramaniam Y., and Cayirci E., (2002), "A survey on sensor networks," IEEE Commun. Mag., vol. 40, pp. 102–114.
[3] Banerjee S. and Mukhopadhyay D., (2006), "Symmetric Key Based Authenticated Querying in Wireless Sensor Networks," In Proceeding of 1st ACM International Conference on Integrated Internet Ad hoc and Sensor Networks.
[4] Benenson Z., Gartner F., and Kesdogan D.,(2004), "User Authentication in sensor network (extended abstract)," In proceeding of informatics, Workshop on Sensor networks.
[5] Das M. L, (2009),"Two-Factor User Authentication in Wireless Sensor Networks," IEEE Transaction on Wireless Communication, Vol.8,No.3, pp. 1086-1090.
[6] He D., Gao Y., Chan S., Chen C. and Bu J., (2010), "An Enhanced Two-Factor User Authentication Scheme in Wireless Sensor Networks," Ad Hoc & Sensor Wireless Networks,vol.0, pp. 1-11.
[7] Khan M. K. and Alghathbar K., (2010), "Cryptanalysis and Security Improvement of 'Two-Factor User Authentication in Wireless Sensor Networks," pp. 2450-2459.
[8] Kumar P., Choudhury A. J., Sain M., Lee S. G., and Lee H. J., (2011), " A Robust User Authentication Framework for Wireless Sensor Networks,", pp. 5020-5046.
[9] Lee-Chun Ko, (2008),"A Novel Dynamic User Authentication Scheme for Wireless Sensor Networks," In the Proceeding of IEEE ISWCS,pp. 608-612.
[10] Lee T. H., (2008) "Simple Dynamic User Authentication Protocols for Wireless Sensor Networks," 2nd International Conference on Sensor Technologies and Application (SENSORCOMM'08), pp. 657-660.
[11] Tseng H. R., Jan R. H., and Yang W., (2007), "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks," IEEE GLOBECOM, pp. 986-990.
[12] Watro R., Kong D., Cuti S-F, Gardiner C., Lynn C. and Kruus P., Tiny PK, (2004),"Securing Sensor Networks with Public Key Technology," Workshop on Security of Ad-hoc and Sensor Networks, Washington, DC,US.
[13] Wong K.H.M., Zheng Y., Cao J., Wang S., (2006) "A Dynamic User Authentication Scheme for Wireless Sensor Networks, " In the proceeding of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06).
[14] Yick J., Mukherjee B., and Ghosal D., (2008), "Wireless sensor network survey," Computer Networks 52, pp. 2292-2330.

AUTHOR'S PROFILE

Chittaranjan Chirom
Email ID : chiromc@yahoo.com

Biodata : My name is Chittaranjan Chirom. I passed my high school leaving certificate exam i.e. 10th exam in 2003 with 73% and all India senior school certificate examination i.e. 12th exam in 2005 with 57%.I got B.Tech. degree in electronics and communication engineering with 8.65c.g.p.a in the year 2009 from Dr. MGR Educational and Research Institute and M.E(communication systems) in the year 2012 in Anna University, Coimbatore in first class with 8.48 c.g.pa.. At present, I am working as guest lecturer in Government Polytechnic, Imphal.
Note: As per the Act No.20 of 2011- Tamil Nadu University Laws (Amendment and Repeal Act), the Anna University of Technology, Chennai, the Anna University of Technology, Coimbatore, the Anna University of Technology, Madurai, the Anna University of Technology, Tiruchirapalli and the Anna University of Technology, Tirunelveli are merged with Anna University, Chennai.