User Authentication using Colors and data security using Armstrong numbers for Wireless Sensor Networks

Shakera Shaikh, Veena Gulhane

***Abstract**: In real world, data security plays an important role where confidentiality, authentication, integrity, non repudiation are given importance.A wireless sensor network(WSN) consisiting of a large number of tiny sensors can be an effective tool for gathering data in diverse kinds of environments.The data collected by each sensor node is communicated to the base station,which forwards the data to the end user. In wireless sensor network data security plays an important role where confidentiality, authentication, integrity, non repudiation are given importance. This paper, propose a User Authentication(UA) scheme for Wireless Sensor Networks (WSNs), which employs RGB color cube algorithm and Armstrong number for data security. The simulation results on NS2 show that Proposed scheme is not only secure but also increase speed of communication than the existing ATTUA scheme.*

Keywords: WSNs, Data Security, Colors, Armstrong Numbers, Authentication.

I. INTRODUCTION

A wireless sensor network[16] is a collection of nodes organized into a cooperative network . Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single omni- directional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Currently, wireless sensor networks are beginning to be deployed at an accelerated pace. It is not unreasonable to expect that in 10-15 years that the world will be covered with wireless sensor networks with access to them via the Internet. This can be considered as the Internet becoming a physical network. This new technology is exciting with unlimited potential for numerous application areas including environmental, medical, military, transportation, entertainment, crisis management, homeland defense, and smart spaces.

Revised Manuscript Received on 30 June 2012

***Correspondence Author(s)

Shakera Shaikh*, Department of Computer Science and Engg, G,H,Raisoni College of Engg, Nagpur, India.

Assist.Prof. Veena Gulhane, Department of Computer Science and Engg, G,H,Raisoni College of Engg, Nagpur, India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license http://creativecommons.org/licenses/by-nc-nd/4.0/

A.Sensor network security issue

Two of the most security-oriented applications of wireless sensor networks are military and medical solutions. Due to the nature of the military, it is obvious that the data (sensed or disseminated) is of a private nature and is required to remain this way to ensure the success of the application. Enemy tracking and targeting are among the most useful applications of wireless sensor networks in military terms[15]. The choice of which security services to implement on a given sensor mainly depends on the type of application and its security requirements. Amongst these we examined:

• Authenticity - it makes possible that the message receiver is capable of verifying the identity the message sender, hence preventing that likely intruder nodes inject malicious data into the network.

• Confidentiality - it ensures that the content of the message is accessed only by authorized nodes.

• Integrity - it guarantees that should a message have its content modified during the transmission, thereceiver is able to identify these alterations.

B. Security requirement

The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior. The security requirements in WSNs include[16]:

• Availability, which ensures that the desired network services are available even in the presence of denial-of-service attacks require configuring the initial duty cycle carefully.
• Authorization, which ensures that only authorized sensors can be involved in providing information to network services.
• Authentication, which ensures that the communication from one node to another node is genuine, that is, a malicious node cannot masquerade as a trusted network node.
• Confidentiality, which ensures that a given message cannot be understood by anyone other than the desired recipients.
• Integrity, which ensures that a message sent from one node to another is not modified by malicious intermediate nodes
• Nonrepudiation, which denotes that a node cannot deny sending a message it has previously sent.

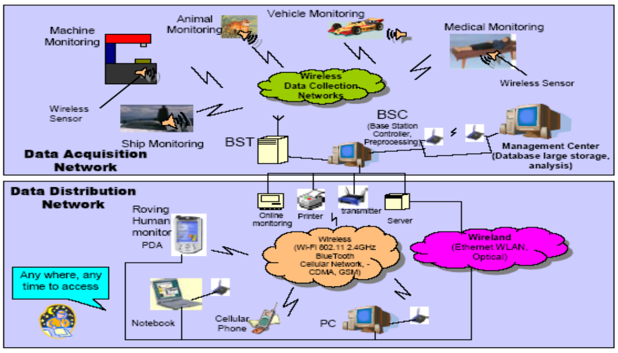

Machine Monitoring
Animal Monitoring
Vehicle Monitoring
Medical Monitoring
Wireless Data Collection Networks
Wireless Sensor
Wireless Sensor
Ship Monitoring
BST
BSC (Base Station Controller, Preprocessing)
Management Center (Database large storage, analysis)
Data Acquisition Network
Data Distribution Network
Roving Human monitor PDA
Online monitoring
Printer
transmitter
Server
Wireless (Wi-Fi 802.11 2.4GHz BlueTooth Cellular Network, - CDMA, GSM)
Wireland (Ethernet WLAN, Optical)
Any where, any time to access
Notebook
Cellular Phone
PC

FIG .1 Wireless sensor Network Scenario

For some special applications of WSNs, such as military surveillance,information gathered is sensitive and must be kept confidential.Therefore in such applications UA is necessary. Health care is a good example of UA application for WSNs: Let's say a WSN offers instantaneous medical data service to subscribed health care employees such as doctors and nurses. Since the confidentiality of the data is important (i.e. patient medical records), only the legitimate users should get a response to their queries. Unauthorized users must be prevented from accessing the mentioned confidential information. Therefore UA is a must in these kinds of networks. UA has been well studied for traditional networks, but those solutions cannot be used for WSNs because of the unique characteristics that WSNs possess.

UA is an intended feature that will increase data security for WSN users and profitability of the network for WS

II. RELATED WORK

UA for WSNs has been used recently in a few other research papers. Solutions for homogenous WSNs were proposed in [2], [3] and [4]. Wong *et al.* [2] proposed a dynamic UA scheme for homogenous WSNs. Later this work was improved by Tseng *etal.* [3] with the following advantages, including resistance of the replay and forgery attacks, reduction of user's password leakage risk, capability of a changeable password, and better efficiency. As discussed in [2], authors claim that weak-password authentication is not suitable for WSNs because it loads the computational overhead to the used cryptography algorithm. In other words the algorithm must be strong enough to compensate for the weakness in the key. Therefore they recommend strong-password authentication for WSNs in which computational load is light owing to the strength in the key. As a result they use SKC throughout the network which is not scalable for a large number of sensor nodes. Although Benenson *et al.*'s scheme [4] uses PKC, it is not practical for WSNs because of the homogenous network structure, meaning that all the power and processing demanding PKC operations are handled on the normal sensor nodes. As a result authentication operations take minutes and batteries of the sensor nodes deplete faster [5]. To our knowledge, in the literature the only heterogeneous approach to the UA in WSNs is the Le *et al.*'s [1] Two Tier User Authentication (TTUA) scheme. In the TTUA scheme, *CH*s are used as a backbone in the network so that the sensed data, after being collected, are transmitted through *CH*s towards the requesting users. Between the *CH*s and the users they issue SKC for authentication. It is practically impossible to scale SKC keys to include a large number of users and sensor nodes, because of the memory limitations. Besides, in SKC excluding existing users from the network and including new users to the network, requires key revoking and key re-distribution, which needs a considerable amount of communication overhead. These are the biggest constraints of the TTUA scheme.Later this work was improved inAdvanced Two Tier User Authentication (TTUA) scheme[1].

In this scheme, WSN consists of basically two elements:
1) *CH*s having high processing capability and long lasting power supplies, such as PDAs. 2) Sensor nodes having low processing capability and limited power supplies, such as MICA2 motes. *CH*s are assumed as trusted gateways to the sensor nodes. Hence they have better power supplies compared to sensor nodes, they are more convenient to run power hungry PKC algorithms. Therefore between *CH*s and users a PKC algorithm, namely ECC, is used for UA purposes. Once a user is authenticated to a *CH* then allowed to access the sensor nodes through that *CH*. Since it is low power demanding, between *CH*s and sensor nodes an SKC algorithm is used. WSN consists of *CH*s and sensor nodes, representing a *Heterogeneous* network structure. ATTUA allows a user to register once and authenticate to the network many times. Users can also change the password anytime at will. We consider wide scale WSN deployed in any variety of environments. In our WSN's architecture, base station (*BS*) is the point of central control, which serves as a trusted key management facility. *BS* is many orders of magnitude more powerful than sensor nodes. Typically, *BS*s have enough battery power to surpass the lifetime of all sensor nodes, sufficient memory to store cryptographic keys, stronger processors, and means for communicating with outside networks. After the deployment, sensor nodes form groups, called clusters. For each cluster, a powerful node is assigned as a *CH*. *CH*s have higher communication power than sensor nodes and therefore possess far more radio transmission coverage. *CH*s can communicate with each other and also with *BS*. In order to protect the keying materials, *CH*s are equipped with tamper-resistant hardware. This assumption is reasonable, hence the number of *CH*s in a heterogeneous WSN is relatively small (e.g., approximately 20- 30 *CH*s for 1,000 sensors), and the cost of such tamper-resistant hardware is small [6]. Users are equipped with portable computing devices, such as laptops, with no power constraints compared to sensor nodes. Users interact with the WSN for data query and retrieval. After processing sensed information; the sensor node either sends the data upon event detection or stores it to serve for the next query.

This scheme has three phases:
1) User registration: User sends a request with his ID encrypted with the public key of the *BS* (*encryptpub keyBS* (*IDU*)) to the *BS* for registration to the WSN. *BS* has the ID list of the legitimate users and provides each legitimate user a certificate. *BS* has private and public key pair (*pri keyBS*, *pub keyBS*) and the certificate is the user's *ID* signed by the *BS*, using the private key (*pri keyBS*). *BS* sends back the certificate to the user. In user authentication phase, with the public key of the *BS* (*pub keyBS*), each *CH* can verify the certificate of the user and extract the *ID* of the user, namely *IDU*.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

2) User authentication: All the communications within the network are routed by the *CH*s.

Let us consider the scenario where the user wants to access data aggregated at a sensor *s* (suppose *A* is *CH*of *s*), and let us also assume that *A* is the closest *CH* in the proximity of the user (intra communications and authentications among *CH*sare beyond the scope of our paper). Then the authentication process includes the following steps:

Step 1) The user sends his certificate *certU* and time stamp *TU* along with the hash value of those concatenated by user ID, *IDU* to *A*: *user* → *A* : *certU*, *TU*,*H*(*certU_TU_IDU*), where _ means concatenation and H stands for hashing algorithm such as SHA-1. Upon receiving an authentication request from the user, *A* first checks whether *TU* is valid, if yes then it can verify the certificate of the user by using the public key of the *BS* (*pub keyBS*) and extract the *ID* of the user, namely *IDU*. Finally *A* verifies the hash value of the user by using the ID of the user.

Step 2) If the verification is successful, *A* sends *s*, users' identification (*IDU*), its identification (*IDA*) and time stamp (*TA*) along with a MAC using its shared pair-wise key (*KA*,*s*) with the sensor *s*, *MAC*(*KA*,*s*, *IDU_IDA_TA*). Upon receiving the message, *s* first checks if *TA* is valid. If yes, it verifies *IDU* and *IDA* by generating a MAC with the shared pair-wise key with *A* (*KA*,*s*) and comparing it with the received MAC. If all of these are successful, then the user is authentic. After successful authentication, sensor *s* is ready to send data to the user. *s* may send a short message to inform the user that he is authenticated via *A*.

System Model

In this proposed scheme Wsn consists of 1) base station with high processing capability.2)sensor nodes having low processing capability with less power.3) Users with no power constraints compared to sensor nodes. Users interact with the WSN for data query and retrieval. After processing sensed information; the sensor node either sends the data upon event detection or stores it to serve for the nextquery.Between user and Base station RGB based cauthentication algorithm is used.And also Armstrong number based security algorithm is used in which 128 bit key is generated using Armstrong number and which is used in aes algorithm foe data encryption and decryption.

A. RGB Based Authentication

The proposed scheme includes two phases: Registration, Authentication.

1)User registration: user module selects onr RGB color value for the user and then find the position of this RGB in the cube and send request with its ID and POS to the base station for registration in Wsn.Base station generate a random number Which is termed as seed .Also the base station module scales the seed value with the Armstrong number and multiply it with the POS it received from the user.It performs MD5 on this product and generate 128 bit key which is used for data security in AES algorithm.Base station send the key and seed to user and store the values in its database.User upon receiving store the POS,SEED,KEY in its database.Figure below depicts the user registration process.

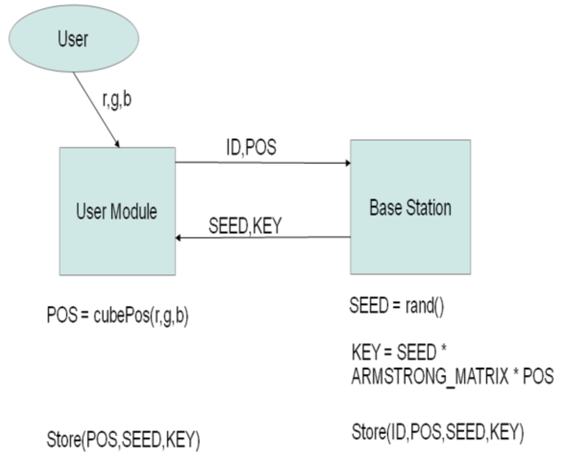


Figure 2.User Registration

*2)User Authentication on Login:*In this phase user find out the new position of RGB using RGB color cube and PRNG in which the user module generate next random number using PRNG in which it uses the seed received form the base station in the registration phase and then offsets its previous RGB POS to NEW_POS with this new SEED_NEW and login with its ID and H[POS_NEW] to the base station.Upon Login request base station also generate the SEED_NEW using PRNG and find out the POS_NEW1 in the RGB cube.If the POS_NEW matches POS_NEW1 the user is authentic. Figure below depicts the user authentication phase.

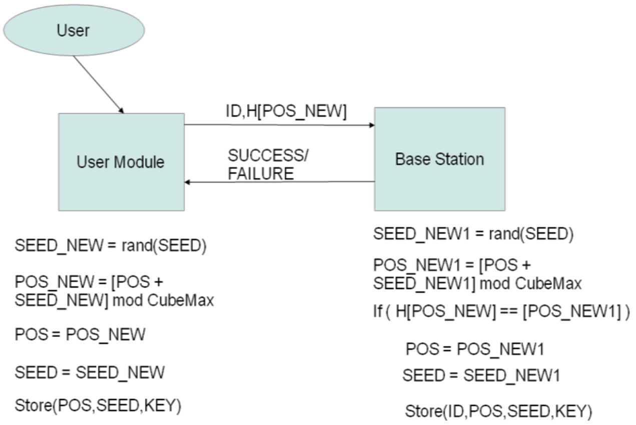


Figure.3 User Authentication

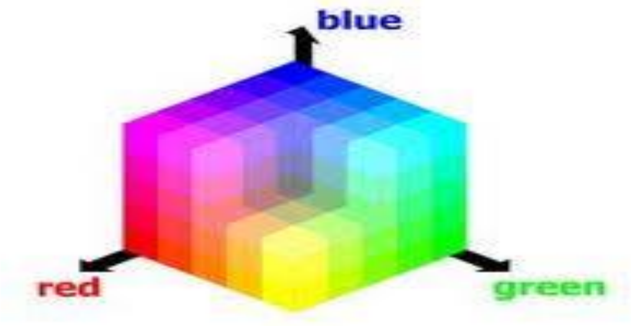


Figure.4 RGB Color Cube

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

The three primary colors of the additive color model are red, green, and blue. This RGB color cube displays smooth transitions between these colors.It has 8 bits per components. 256 * 256 * 256 number of possible colours Each colour represented by a number in the cube(POS):
POS = r + (g*256) + (b*256*256)

B. Pseudo RNG

Uses 'seed' state. A PRNG can be started from an arbitrary starting state using a seed state. It will always produce the same sequence thereafter when initialized with that state. The period of a PRNG is defined as the maximum over all starting states of the length of the repetition-free prefix of the sequence. The period is bounded by the size of the state, measured in bits. However, since the length of the period potentially doubles with each bit of 'state' added, it is easy to build PRNGs with periods long enough for many practical applications Uniformly distributed random numbers. If 2 parties use same seed on the same PRNG, it will deterministically give the same next number.
$X_{n+1} = F(X_n)$

C. Data Security

Upon successful authentication base station encrypts the requested data with the key generated using Armstrong number in AES aloritnhm and send data to the user then user decrypt data uing AES algorithm with the key generated using Armstrong number.

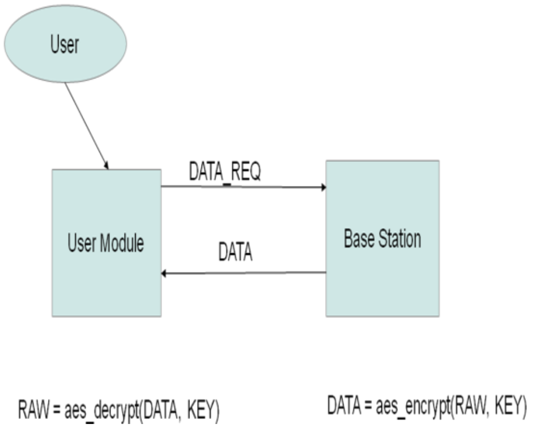


Figure.5 Data Encryption Decryption

IV. Security Analysis

1)Level1
i)POS_NEW is never sent as plain number, rather its hash is sent.

2)Level2
i)Attacker cannot simply steal H[POS_NEW] and send (i.e. replay attack), because that becomes obsolete. Attacker will have to guess the next H[POS_NEW].
ii)POS_NEW = f(POS, SEED)
iii)SEED is never sent on wire
iv)Larger the SEED length, harder to guess

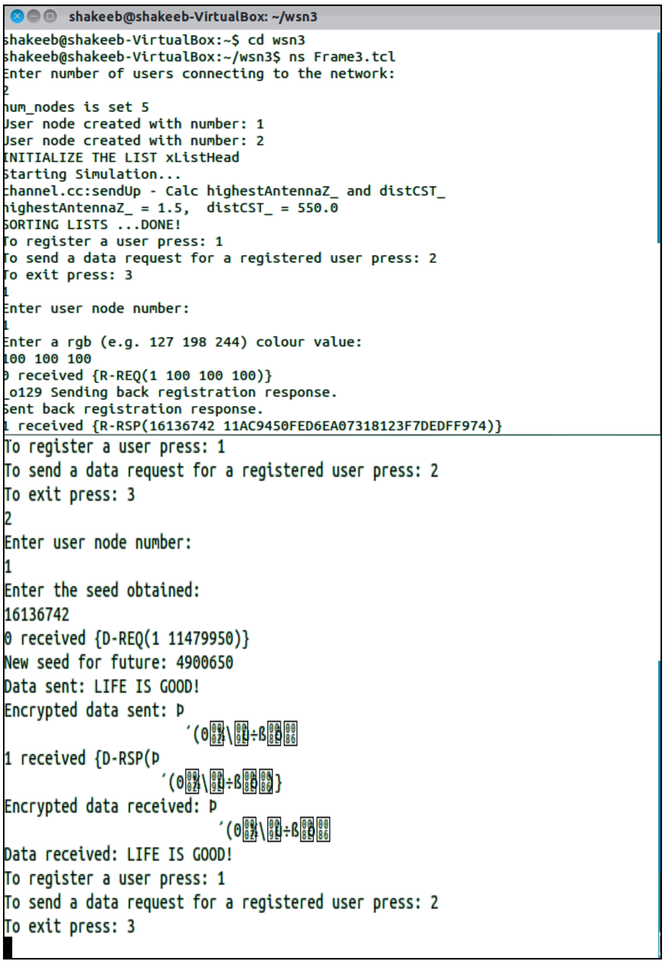
V.PERFORMANCE COMPARISION

	RGB based authentication	ATTUA
Average time required for registration	0.000173 seconds	0.166563628 seconds
Average bytes required for registration	67 Bytes	68 Bytes [256 bit public/private key]
Average time required for login	0.000152 seconds	0.002171226 seconds
Average bytes required for login	40 Bytes	104 Bytes

VI. SIMULATION PARAMETERS

The RGB based user authentication scheme is implemented on NS2.34 with 5 sensor nodes randomly distributed over 670x670m^2. Number of users 10 and one base station node..Simulation time1099.000703seconds .

VII. RESULTS:



```
hakeeb@shakeeb-VirtualBox:~$ cd wsn3
hakeeb@shakeeb-VirtualBox:~/wsn3$ ns Frame3.tcl
nter number of users connecting to the network:

um_nodes is set 5
ser node created with number: 1
ser node created with number: 2
NITIALIZE THE LIST xListHead
tarting Simulation...
hannel.cc:sendUp - Calc highestAntennaZ_ and distCST_
ighestAntennaZ_ = 1.5,  distCST_ = 550.0
ORTING LISTS ...DONE!
o register a user press: 1
o send a data request for a registered user press: 2
o exit press: 3

nter user node number:

nter a rgb (e.g. 127 198 244) colour value:
00 100 100
 received {R-REQ(1 100 100 100)}
o129 Sending back registration response.
ent back registration response.
 received {R-RSP(16136742 11AC9450FED6EA07318123F7DEDFF974)}
To register a user press: 1
To send a data request for a registered user press: 2
To exit press: 3
2
Enter user node number:
1
Enter the seed obtained:
16136742
0 received {D-REQ(1 11479950)}
New seed for future: 4900650
Data sent: LIFE IS GOOD!
Encrypted data sent: Þ
                        ´(0▯\▯÷ß▯▯
1 received {D-RSP(Þ
                     ´(0▯\▯÷ß▯▯}
Encrypted data received: Þ
                           ´(0▯\▯÷ß▯▯
Data received: LIFE IS GOOD!
To register a user press: 1
To send a data request for a registered user press: 2
To exit press: 3
```

Figure.6 Output of the RGB based scheme

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

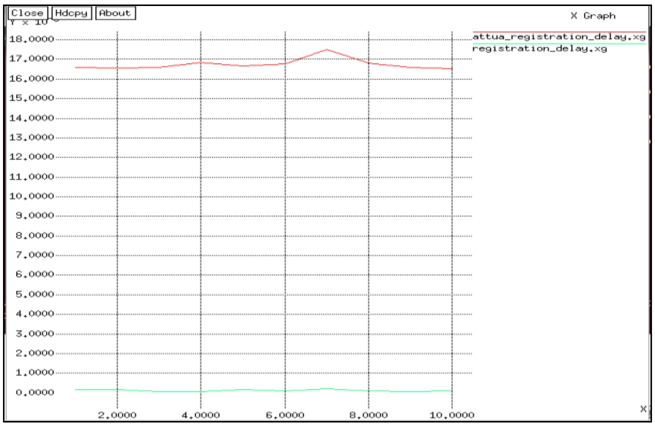


Figure .7 Average Time required for registration

The above graph indicates the average time required for a user to register to the base station.On x-axis is the user number and on y-axis is the time in seconds.The graph show that the proposed scheme requires less time for registration than the ATTUA scheme.

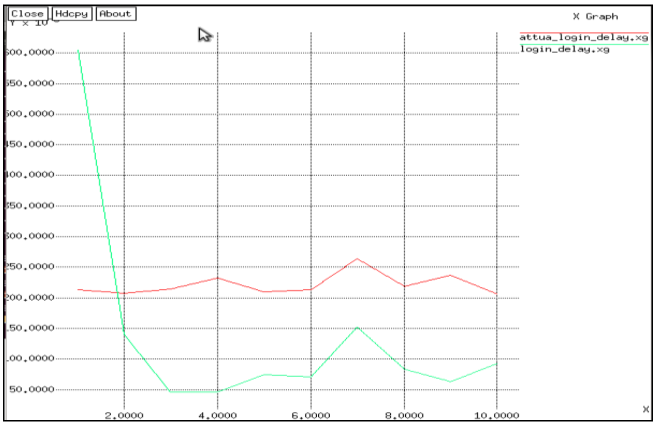


Figure.8 Average Time required for Login

The above graph indicates the average time required for a user to login .On x-axis is the user number and on y-axis is the time in seconds.The graph show that the proposed scheme requires less time for login than the ATTUA scheme.

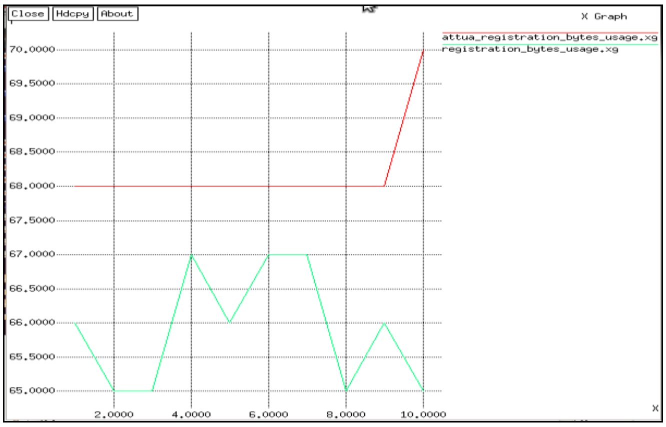


Figure.9 Average Bytes required for registration

The above graph indicates the average number of bytes required for a user for registration. .On x-axis is the user number and on y-axis number of bytes..The graph show that the proposed scheme consume less bytes for registration than the ATTUA scheme

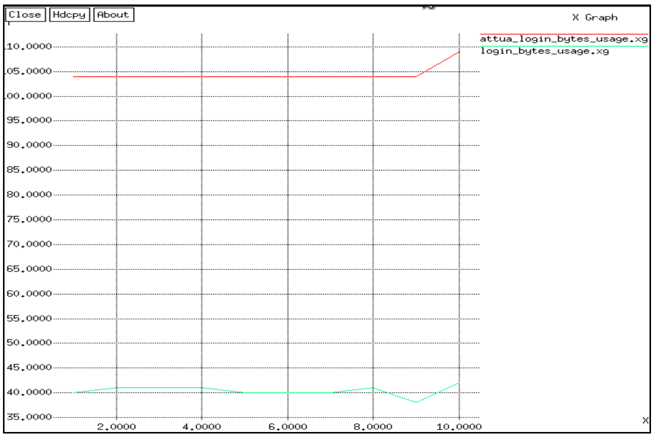


Figure .10 Average Bytes required for Login

The above graph indicates the average bytes required for login .On x-axis is the user number and on y-axis is the number of bytes.The graph show that the proposed scheme consume less bytes for login than the ATTUA scheme.

IX. CONCLUSION

In this paper we propose a user authentication scheme for wireless sensor network named RGB based authentication scheme.This scheme provides sufficient security for sensor nodes having less processing capability. Simulation results on NS2[12] have shown that the RGB based authentication scheme requires less time for registration and login also bytes consumed by the proposed scheme is less than than the existing scheme.

REFERENCES

1. Ismail Butun and Ravi Sankar,2011." Advanced Two Tier User Authentication Scheme for Heterogeneous Wireless Sensor Networks". 2nd IEEE CCNC Research Student Workshop.
2. X.H. Le, S. Lee, and Y.K. Lee. "Two-Tier User Authentication Scheme for Heterogeneous Sensor Networks." the 5th IEEE International Conference on Distributed Computing in Sensor Systems, (DCOSS '09),Marina Del Rey, California, USA, June 8-10, 2009.
3. K.H.M. Wong, Y. Zheng, J. Cao, and S. Wang. "A dynamic user authentication scheme for wireless sensor networks." IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006.
4. H.R. Tseng, R.H. Jan, and W. Yang. "An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks." IEEE Global Communications Conference, (GLOBECOM 2007), USA, November 2007, pp. 986-990.
5. Z. Benenson, N. Gedicke, and O. Raivio, "Realizing robust user authentication in sensor networks." in Worshop on Real-World Wireless Sensor Networks, 2005
6. Binod Vaidya, Jorge Sá Silva, Joel J. P. C. Rodrigues,2009." Robust Dynamic User Authentication Scheme for Wireless Sensor Networks"proceeding of the 5th ACM symposium on QOS and security for wireless and mobile networks.
7. Omar Cheikhrouhou1,2, Anis Koubaa3,4, Manel Boujelbenl, Mohamed Abid1,2010." A Lightweight User Authentication Scheme forWireless Sensor Networks" International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

8. C. Jiang, B. Li, and H. Xu, “An efficient scheme for user authentication in wireless sensor networks” in 21st International Conference on Advanced Information Networking and Applications Workshops
9. Orhanou, G.El Hajji, S.; Bentaleb, 2011. “EPS AES-based confidentiality and integrity algorithms: Complexity study”.International conference on Multimedia communication and computing.
10. Hyeopgeon Lee, Kyounghwa Lee, Yongtae Shin,2010. “Implementation and Performance Analysis of AES-128 CBC algorithm in WSNs”.
11. Hu, Zhihua,2011. “Progress on advanced encryption standard”. International conference on Intelligence Science and Information Engineering.China.
12. Vishnu, M.B.; Tiong, S.K.; Zaini, M.; Koh, S.P,2008. “Security enhancement of digital motion image transmission using hybrid AES-DES algorithm”14 Asia pacific conference on communications.
13. Wong, M. M.; Wong, M. L. D.; Nandi, A. K.; Hijazin,2011. “Construction of Optimum Composite Field Architecture for Compact High-Throughput AES S-Boxes” .International conference on Integration(Vlsi Systems)
14. Advanced Encryption Standard”,2001.Federal Information Processing Standard Publications.
15. Pathan, A.S.K. Dept. of Comput. Engg., Kyung Hee Univ., Seoul Hyung-Woo Lee ; Choong Seon Hong **“**Security in wireless sensor networks: issues and challenges”, Advanced Communication Technology, 2006. ICACT 2006,
16. F. L. LEWIS .“Wireles sensor networks” Associate Director for Research Head, Advanced Controls, Sensors, and MEMS Group Automation and Robotics Research Institute The University of Texas at Arlington,2004
17. NS-2-Network Simulator and Emulator, http://www.isi.edu/nsnam/ns

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

© Copyright: All rights reserved.