Review of Information Engineering and Applications
2014 Vol. 1, No. 1, 24-38.
ISSN(e): 2409-6539
ISSN(p): 2412-3676
DOI: 10.18488/journal.79/2014.1.1/79.1.24.38

AN UNIFIED APPROACH BY IMPLEMENTING THE SECURED AUTHENTICATION PROTOCOL SCHEME IN WIRELESS SENSOR NETWORKS

R. Sujatha[1]† --- M. Lawanya[2]

[1]*Principal, Holy Grace Academy of Engineering, Thrissur, Kerala, India*

[2]*Database Developer, Nabko systems and communications Pvt ltd, Bangalore India*

ABSTRACT

Wireless Sensor Networks (WSN) is an ad-hoc mobile network and is highly vulnerable to attacks because, it consists of various resource-constrained devices and they communicate via wireless links. Security of group communication for large mobile wireless sensor network hinges on efficient authentication protocol scheme. Consequently, one of the most primary challenge, on endow with the security services in sensor nodes are key distribution. Secure communications in wireless sensor networks are critical. As the wireless medium is characterized by its lossy nature, reliable communication cannot be assumed with pair-wise keys, LOCK (Localized Combinatorial Keying) and Structured Graphs etc. Therefore, security with key distribution is a good factor considered in wireless sensor network communications. The only requirement for a user is to send information in a reliable manner to the destination; this will be provided only with the security. In this regard, a novel secured authentication protocol scheme with finger-print scheme provides full security and very good resilience is proposed. It also has low transaction overhead and reduced less space overhead. This novel method produces good improvements in the functionality of security.

Keywords: SAP (Secured Authentication Protocol), Authentication, WSN (Wireless Sensor Networks), Security, MAC (Message Authentication Code), Authentication protocol, Image based authentication protocol, Finger-print authentication.

Contribution/ Originality

This study is one of very few studies which have investigated in the area of Authentication in Wireless Sensor Networks. Major threats are viewed and addressed with the dynamic password system. With this dynamic methodology hacking of text-based password is not feasible.

1. INTRODUCTION

Wireless Sensor Networks provide a trouble-free, fiscal approach for the [1] exploitation of disseminated scrutinize and control devices, avoiding the exclusive retrofit necessary in wired

† Corresponding author

systems. The interest towards wireless sensor networks is simply by thinking in an essential manner with a large number of miniature sensor self-powered nodes which acquire information and to detect special measures and communicate in a wireless trend, [2] with the goal of furnishing their processed data to a base station.

A typical WSN consists of hundreds or even thousands of small and resource-constrained sensor nodes. These sensor nodes are distributed and organized in uncontrollable environment for the collection of security-sensitive information. Individual sensor nodes rely on multi-hop wireless communication to deliver the sensed data to a remote base station. In an essential WSN situation, resource limitation, wireless communication, security-sensitive data, irrepressible environment, and even distributed deployment are all vulnerabilities. These susceptible threats make WSNs suffer from an astonishing number of security threats. WSNs can only be used in the grave applications after the potential security threats are eliminated.

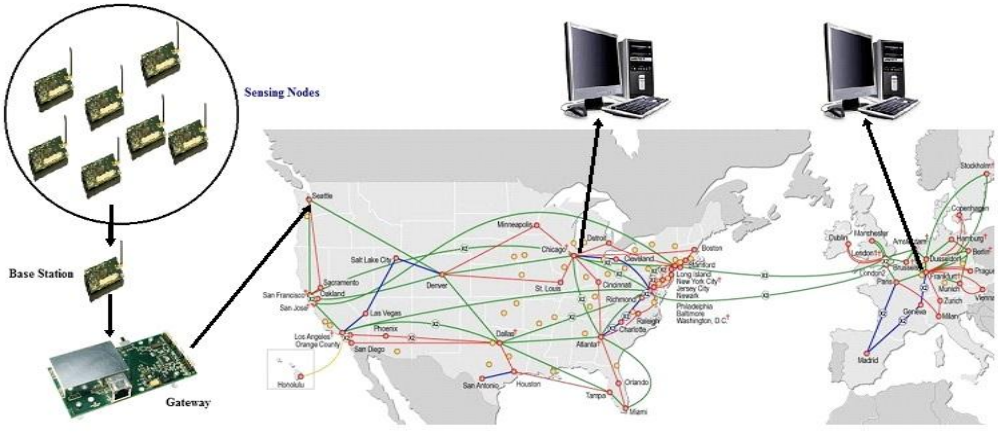


Fig-1.1. A Representation of Base Station and Gateways in WSN.

The future of WSNs is very potential; WSNs will not be successfully organized if security, reliability and privacy issues are not addressed adequately. These issues become more important because WSNs are usually used for very significant applications. Additionally,[3] WSNs are very susceptible and thus striking to attacks because of their limited prices and human-unattended exploitation. A representation of Base station and its Gateways in WSN is presented in Fig. 1.1.As sensor networks are mostly deployed in human-unattended environments for critical intellect measurements, the authentication of the data source as well as the data are grave concerns. Appropriate authentication mechanisms can provide WSNs with both sensor and user identification facility, can protect the reliability and originality of critical data, and can forbid and identify impersonating attack. Traditionally Symmetric-key Authentication, can be provided as message authentication code, which ensures integrity, where as public key combination will be in the form digital signature. In Section 2, Security threats in WSN are discussed and in Section 3, related works are discussed with their drawbacks. Section 4 discusses the overview of Proposed SAP System in WSN. In section 5, implementation details related to the system are presented. Conclusion is given in section 6.

2. SECURITY THREATS IN WSN

An assailant may disrupt the communication to break secret key and extract classified data from the secured messages exchanged between communicating nodes. With the key authorisation the assailant tries to be active as legitimate node in order to capture the private information from other nodes. From this, the assailants may understand the message pattern and guess the secret key Classifications of attacks on WSN are,

A. Passive Information Gathering and Message Corruption

Passive information gathering and message corruption are the simplest attacks that can take place in WSN. If information is not encrypted, an adversary can listen to the communication passively. Passive information gathering can be classified as interception carried out by an outside node.

B. Node Concession

An adversary may control a node by negotiating it's limitation in its system software. Through this, they can manipulate the accurate data, by getting access to the secured information including cryptographic keys that are stored in the node.

C. Selective Forwarding

In this, an assailant compromises a normal node or makes use of an outsider malicious node so as to make a black hole in the target sensor network. The malicious node purposely drops data packets in order to interrupt working of the target sensor network or make the custom node refuses to forward the damage content.

D. Sinkhole Attacks

The purpose of an adversary in sinkhole attacks is to entice the network towards compromised malicious node, which creates sinkhole in the target sensor networks. If the malicious node is close to the base station, then selective forwarding and sinkhole tamper the data effectively.

C. Sybil Attacks

In this attack, a node is threatened by fake identities in the sensor network. In doing so, it can illegitimately embezzle other nodes' identities or it can try to formulate new identities itself. Basically, Sybil attacks reduce effectiveness of fault tolerant schemes like distributed storage and also affect routing algorithms.

D. DoS (Denial of Service) Attacks

Adversary's aim in dos attack is to formulate the resource unavailable or generating traffic to the legitimate users by interrupting the communication between sensor nodes. Typically DoS attacks occur at the physical layer of WSN. As a result, most of the attacks can be evade by

replacing with a highly effective node authentication. Strength of node authentication depends upon the underlying key management scheme.

To defend [4] against false data injection, authenticity of the sender must be checked so that sensors will not listen to unauthorized nodes. Modification of a message is detected by checking integrity of the message. Message reliability can be identified by information variation checking. To ensure privacy, the information enclosed in the message should not be exhibited to any node apart from sender and receiver. To ensure authentication a secured authentication scheme is followed among sensor nodes. For the distribution of this kind of security scheme a Secured Authentication Protocol scheme have been proposed.

3. RELATED WORK

In [5] several attacks on four layers of OSI model are discussed and security mechanism is described to prevent attack in network layer i.e. wormhole attack. In wormhole attack two or more malicious nodes construct a covert channel which attracts the traffic towards itself by depicting a low latency link and then start dropping and replaying packets in the multi-path route. This paper proposes promiscuous mode method to detect and isolate the malicious node during wormhole attack by using Ad-hoc on demand distance vector routing protocol (AODV) with omni-directional antenna. The methodology implemented notifies that the nodes which are not participating in multi-path routing generates an alarm message during delay and then detects and isolate the malicious node from network.

In [6] the networks can consist of everything from smaller number of nodes for sparsely populated networks, up to 100's of thousands of nodes in densely populated networks. Watchdog algorithm is in existence is unable to catch the misbehaving sensors due to which network traffic is being upset. The goal is to create IDS such that the throughput of the system must be efficiently increased and PDR must be improved. Two algorithms are implemented simultaneously to detect the nodes which acting as true node and fake other true nodes to be misbehaving. This approach is implemented in the watchdog mechanism to improve the performance, throughput, accuracy, energy efficiency at low cost and less time consuming.

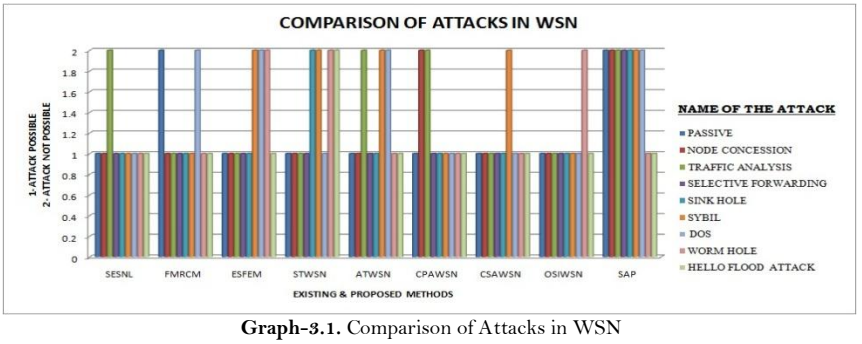
In [7] et. al. described that networks are deployed in variety of fields in unattended way and this makes them prone to different types of attacks. Limited resources, like battery power, memory and wireless communication channel enhance difficulty of implementation of security in wireless sensor networks. The approach have proposed in this framework for implementing security in energy efficient way and provide various symmetric encryption methods for fast processing with small memory consumption and less storage requirement.

In [8] described a modified version of blast technique. Consider a network structure of randomly deployed sensor nodes. The network is divided into two set of nodes called viz. ordinary and special nodes. Special nodes are selected at random as a set of nodes in the area surrounding the sink node covering a certain range. Sink node can be positioned anywhere within this set and it is not essentially at the centre. But, the condition is that it must lie within

coverage area of these special nodes. The whole network is constructed in the form of clusters using some good clustering mechanism. Many factors are taken into account for selecting a cluster head like battery life, transmission power, location, etc. The main object of a clustering algorithm is extension of network life span, reduced energy consumption by each sensor and use of data aggregation to trim down number of messages.

In [9] described that some security concerns must be addressed from the beginning of the system design. Securely communication among sensor nodes is a fundamental challenge for providing security services in WSNs. Many researchers have tried to provide security by using symmetric key cryptography, but thinking that public key steaganography are feasible to implement in these networks because they are provided with more resources. This paper tends to investigate the security related issues and challenges in wireless sensor networks. It is to identify the security threats, discuss the proposed security mechanisms for wireless sensor networks and also present the obstacles and the requirements in the sensor security, classify many of the current attacks, and finally list their corresponding defensive measures.

As a result, with the use of highly effective node authentication, the majority of the attacks can be evaded. Strength of node authentication depends upon the underlying key management scheme. To defend [4] against false data injection, authenticity of the sender must be checked so that sensors will not listen to unauthorized nodes. Comparison of existing methods with the proposed method is to infer that this SAP model (proposed) is designed with impossible of attacks listed in WSN. The comparison graph is represented in Graph 3.1.



Graph-3.1. Comparison of Attacks in WSN

The message send is encrypted with a key that is shared by sender and receiver. Keys play a vital role in recognizing security services like: legitimacy, reliability, privacy etc. To ensure authentication a secured authentication scheme is followed among sensor nodes. Intended for this kind of security scheme a secured authentication protocol scheme have been projected.

4. INGENIOUS AUTHENTICATION SCHEME USING SAP IN WSN

This system involves the use of authentication mechanism for wireless sensor networks that minimizes the hacking by the attackers. The core conceive of this novel scheme is that 'Instead of remembering a sequence of characters as password, users have to remember a sequence of patterns as their password'.

A. Introduction

The development and maintenance of end user interface software in WSN are demanding. The interface development environments provide facilities that allow individual components within an interface to be constructed without recourse to programming. But the behaviour of end user interfaces is generally implemented by complex, hand crafted software systems. The dynamic creative patterns can be used to provide an organisational structure for end user interface software. Changing an existing interface to reflect changing requirements and to take account of end user feedback is a laborious and often somewhat ad-hoc process.

The system should provide flexibility not only to the individuals but also across different groups. A groupware infrastructure is defined by three dimensions: a) Communication b) Collaboration and c) Coordination. Protected substantiation system is relevant for a computer system to process information with different sensitivities (i.e. classification of information at different levels) to permit simultaneous access by users with different security clearance and to prevent end users from obtaining access to information for which they lack authorization. Secured Authentication Scheme has two goals: First goal is to prevent unauthorized personnel from accessing information. Subsequent goal is to prevent unconstitutional personnel from declassifying information.

The solution presented here offers flexibility both at the group level and at the application level. At the group level, the shared workspace can be adapted by loading collaboration-specific that incorporate the collaboration and coordination dimensions into the end user interface. At the application level, the end user can choose between multiple image modalities to interact with the application. In this authentication scheme, end users choose their passwords from the finger-print scanner and flexible user interface image patterns. User has to enter random patterns as their passwords for the chosen flexible user interface image patterns. At every sequence of iteration these random patterns are varied and associated with hidden characters (assigned to image patterns) at run time. Every registered end user has a hash value and it should be compared with generated hash vale at login time, to see if it matches then authentication granted to the end user otherwise denied. This authentication scheme overcomes the identified drawbacks of existing systems.

B. Framework of the SAP Scheme for WSN

Flexibility is the requirement of most human users in network security in the present development for WSN. The need of user's flexibility is provided in this framework of Secured Authentication Protocol Scheme. This is a scheme with both finger-print and text-based authentication using flexible user interface image patterns. This vision of 'remembering and recollecting picture patterns than text patterns' is incorporated to authenticate the end users in a memorized way.

Locating the sensor node in WSN and accomplishing the task of providing security to the sensor node through SAP Scheme is assumed and presented. Different kind of flexible user

interface image patterns and random patterns can be used in this system for various scenarios to provide secured authentication in WSN. This flexible user interface image patterns does not provide any conflict between the systems used in various WSN applications.

C. Levels of Authentication in SAP for WSN

These systems utilize the authentication mechanism and a server that reduce the hacking by the intruder. It monitors the clock cycle process effectively. The security level is emphasized with two levels of authentication system. The flow-diagram of WSN-SAP Authentication System is represented in Figure. 4.1.Two levels of authentication phases are involved in this system; they are a) Finger-print Authentication and b) Dynamic Random Patterns with Flexible User Interface Image Patterns Authentication System.

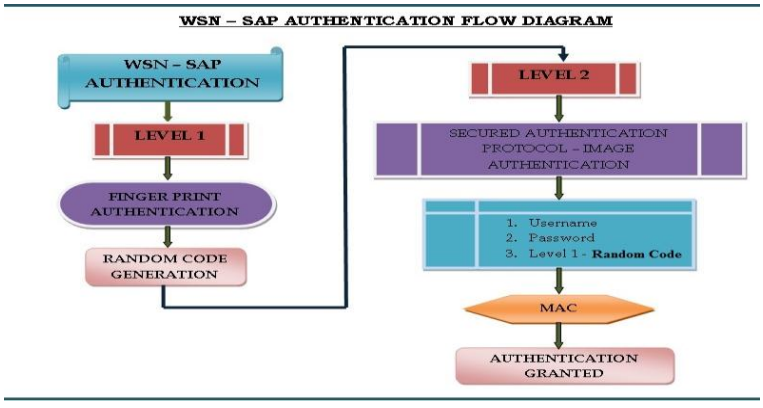


Figure-4.1 WSN-SAP Authentication System Flow-Diagram

1. Finger-Print Authentication

In the first level of authentication process the end user has to get authentication through finger-print method. After the finger-print login a random code gets generated. This random code has sent to the second level of authentication process. Every time a new random code gets generated for each end user and it will be sent to dynamic random patterns array.

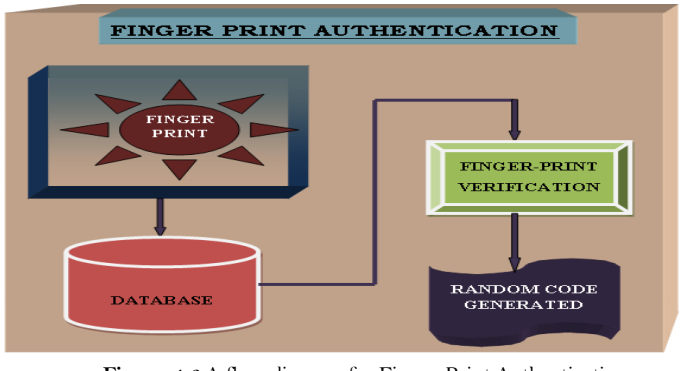


Figure-4.2.A flow-diagram for Finger-Print Authentication.

Figure.4.2 show the flow-diagram for Finger-Print Authentication system. End users finger-prints are kept in the database for future verification process. After verification of finger-prints from the database an end user will be provided with random code. This random code is utilized for second level of authentication process.

2. Dynamic Random Patterns with Flexible User-Interface Image Patterns Authentication System

The customary view of tenable authentication is one of ensuring that information at a high security categorization cannot flow down to a lower security categorization.

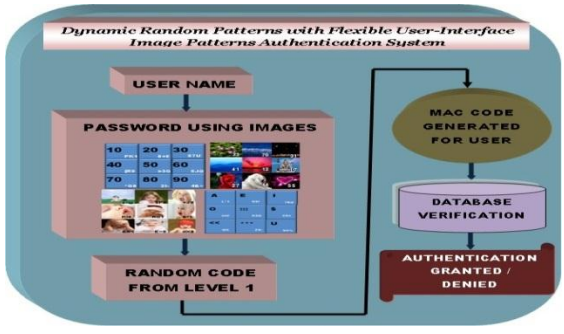


Figure-4.3. Flow-Diagram for Dynamic Random Patterns with Flexible User-Interface Image Patterns Authentication System.

After I level of finger-print authentication each end user enters into the II level with random code. In this II level of Dynamic Random Patterns with Flexible User-Interface Image Patterns Authentication System each end user will obtain a MAC code. The flow diagram is illustrated in Figure. 4.3. In this II level each end user should process their password with images. From a set of flexible user-interface image patterns the end user has to select set of image patterns as their password. When selecting image patterns the end user has to enter the dynamic random patterns in the password area.

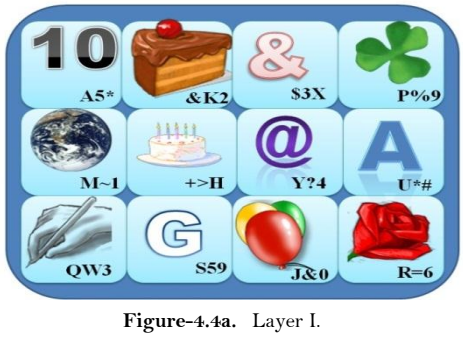


Figure-4.4a. Layer I.

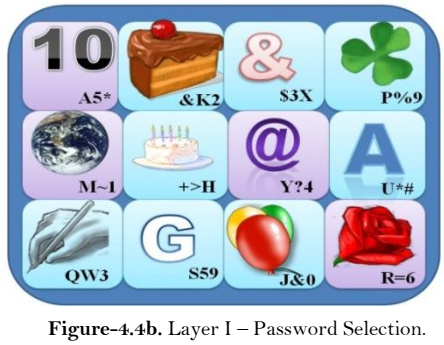


Figure-4.4b. Layer I – Password Selection.

Consider that the end user choosing password from Figure. 4.4a as ***"10GlobeRose@"*** images. The end users password selection is represented in Figure. 4.4b. Now the end user has

to enter the password as random patterns, which is ***"A5*M~1R=6Y?4".*** On the next time if the same end user tries for login it is possible with new dynamic random patterns and image patterns only. The new set of patterns with layer II is represented in Figure. 4.4c. The password selection for layer II is represented in Figure. 4.4d, the end user has to enter the password as ***"J&0%*U"LO6F$"***.

On every registration and login by an end user the password entry is dynamic. This SAP system provides dynamic random patterns to ensure the security level of process.

Figure-4.4c. Layer II.

Figure.4.4d. Layer II – Password Selection.

Figure-4.4. Dynamic Random Patterns with Flexible user-interface image patterns.

The authentication process is dynamic in nature in this mechanism, which gives an additional advantage to pursue the process. End users may have different views about image patterns. One personality may like car images, another may like personality images, another may be flowers etc. These statuses of different image patterns bring about new ventures in the authentication circumstances. According to the end user needs the change in image patterns is required. This is accomplished by having different set of image patterns in the authentication scenario. One kind of representation made with baby images, i.e. known baby images also comprised. It is represented in Figure. 4.5.

Figure-4.5. Dynamic Random Patterns with Flexible user-interface image patterns using baby images.

Normally the image patterns in authentication scheme which varies according to the applications. Here in this set of image patterns the end user may select their own selection of babies from the displayed baby set images.

Another advantage of having this kind of personalities in this scheme is to add same personality images with different stills. The end user makes a remembrance of variety of stills that he/she likes in the image patterns and select as password image patterns.

All this image patterns will be shown to the end users on iteration basis. On each iteration the dynamic random patterns and varied image patterns displayed on the end user screen. From this visual the end user has to select the password image patterns. Each password image pattern (i.e. corresponding random pattern) is associated with Hidden numbers. If the end user choosing the password from 1ST row, first four images, then he/she has to enter the random patterns as *N&KU8&@1$B2. Now this random pattern is associated with Password Image Pattern Numbers (I1, I2, I3 and I4) and Hidden Characters (2G5, K+@, 58* and PM9). Finally, a MAC code gets generated for this selected password. It will be sent to database for future authentication process. The representation of random patterns, image patterns and hidden characters is presented in Table I.

The digits (n value) include alphabets (26), numbers (0-9) and special characters (32), which create 8320! (26 x 10 x 32) combinations of characters occurred for display. This combination of characters is set with 3 digit process in this Secured Authentication Protocol Scheme for Wireless Sensor Networks implementation, so in total *8320! x 3* (each digit 8320! combinations of characters) = *8.55583707135835037295325701362 87e+29004* combinations made in this dynamic mechanism. According to the number of digits taken, possible combination of characters was framed and utilized in the display system.

Table-1. Dynamic Random Patterns, Password Image Pattern Numbers and Hidden Characters Are Associated In Iterations

Password Image Pattern Numbers	Hidden Characters	Dynamic Random Patterns			
		Iteration I	Iteration II	...	Iteration N
I1	2G5	*N&	890	...	UIO
I2	K+@	KU8	JHG	...	43*
I3	58*	&@1	%&9	...	@#$
I4	PM9	$B2	$39	...	^%K
I5	@1Q	@R6	H7&	...	&Z&
I6	SD=	W@!	R^3	...	@9P
I7	UE8	*ER	$X2	...	T6B
I8	469	?%2	?+1	...	8#2
:	:	:	:	...	:
IN-1	J7*	4TW	Y3&	...	495
IN	V#5	=+2	F&&	...	0G#

Possible combinations are framed and displayed for end user entry on the display screen. Thus usage of alphabets, numbers and special characters in random patterns provide much security than other password systems. This arrangement makes hacker incapable to intrude the password given by the end user.

5. IMPLEMENTATION OF SAP SCHEME IN WSN

SAP implemented with the design of random patterns in Wireless Sensor Networks. The end user has to choose password as image patterns. He / she should provide the random patterns in the password area. While entering random patterns in the password area, it will be hidden. Only bullet marks will be displayed. Here the system is represented as a sample 3 x 3 matrix set of password image patterns. It is demonstrated in Figure 5.1.

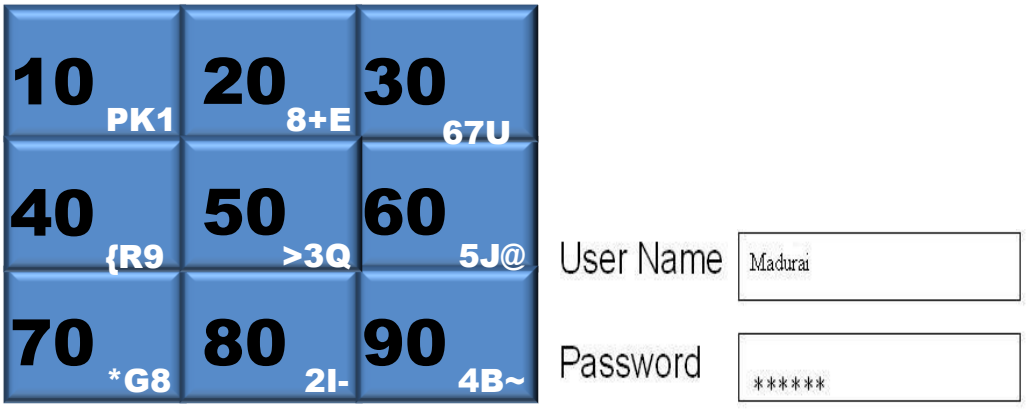


Figure-5.1. A sample 3 x 3 SAP for WSN using Random Pattern based Flexible User Interface Image Patterns.

Due to the end user viability an implementation of SAP for WSN made with finger-print, characters, numbers and special characters represented as password image patterns along with 3 digits random numbers is represented in Figure 5.2 – 5.10 respectively. This way of incorporating characters (A-Z, a-z), numbers (0-9), and special characters (28) in image patterns and random numbers reduces the guess ability of password from malicious users. The sequence of characters, numbers, and special characters occurs for each digit in random makes an added advantage for the protocol scheme, which unable to predict the password in this WSN process.

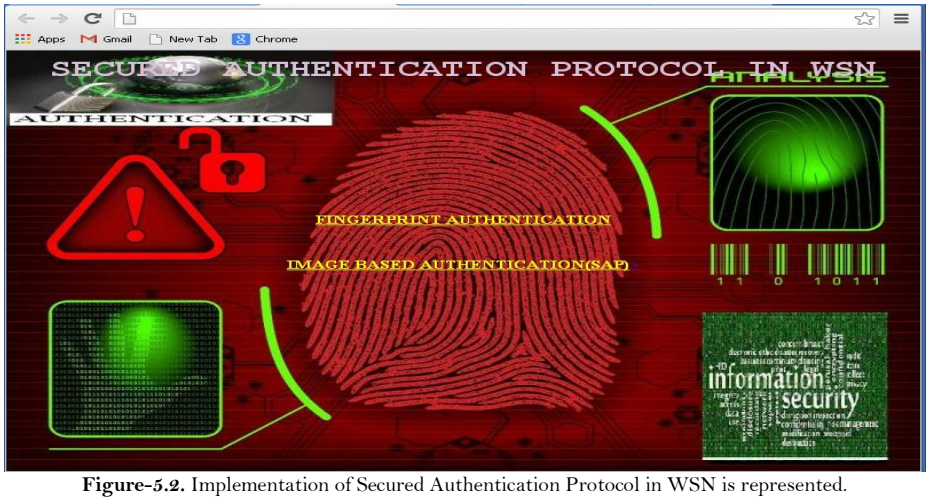


Figure-5.2. Implementation of Secured Authentication Protocol in WSN is represented.

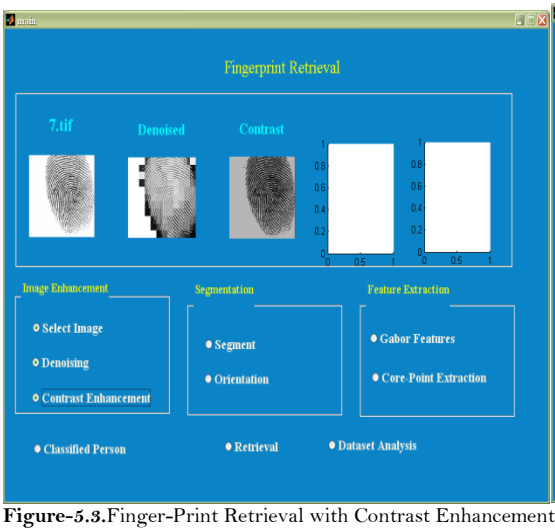


Figure-5.3. Finger-Print Retrieval with Contrast Enhancement

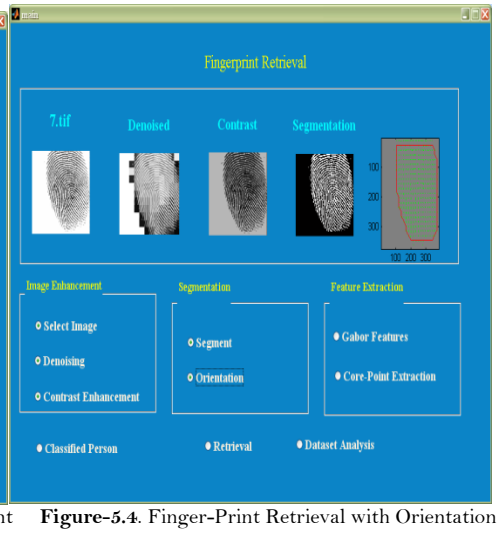


Figure-5.4. Finger-Print Retrieval with Orientation

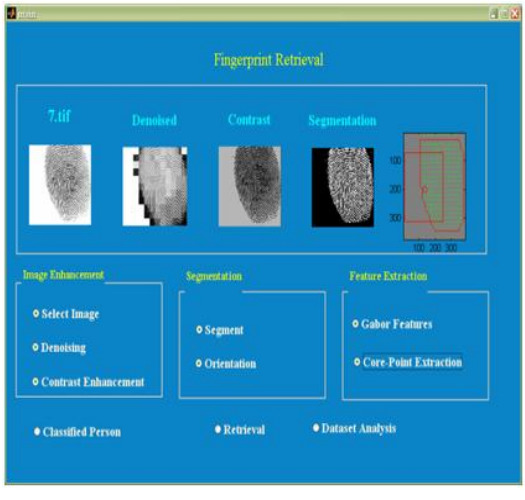


Figure-5.5. Finger-Print Retrieval with Core Point Extraction

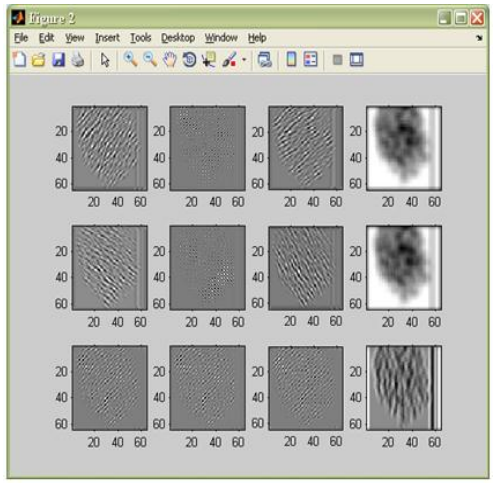


Figure-5.6. Gabor Filtered Finger-Print Images in 12 Directions

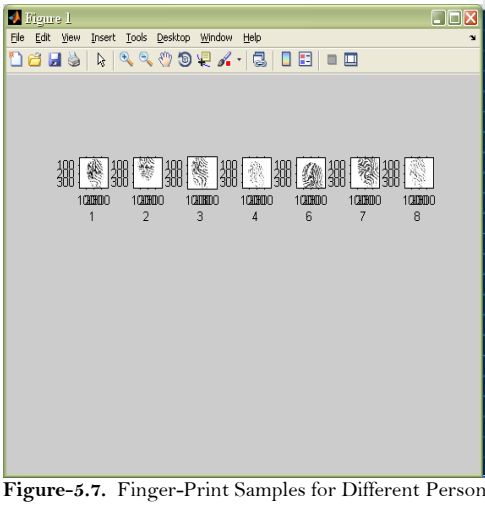


Figure-5.7. Finger-Print Samples for Different Persons

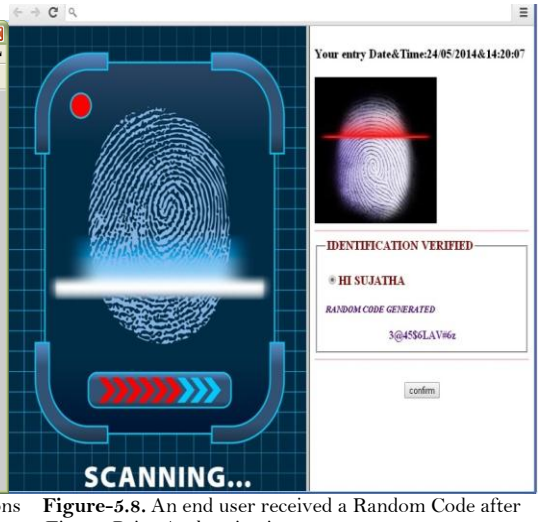


Figure-5.8. An end user received a Random Code after Finger-Print Authentication

When the end user entered into this scheme he/she should depart with finger-print authentication and followed with image-based authentication (i.e. Secured Authentication Protocol model). In the finger-print authentication process one of the feature helps to improve selection of an image with orientations. To extract useful features from an image, a set of Gabor filters with different frequencies and orientations are essential. The purpose of the Gabor filtering stage is to enhance the clarity of the ridge structures while reducing noise in the image. Gabor filtration removes noise while preserving ridge structures and providing information contained in a particular direction in the image [9]. The Gabor filters optimally capture both local orientation and frequency information from a finger-print image.

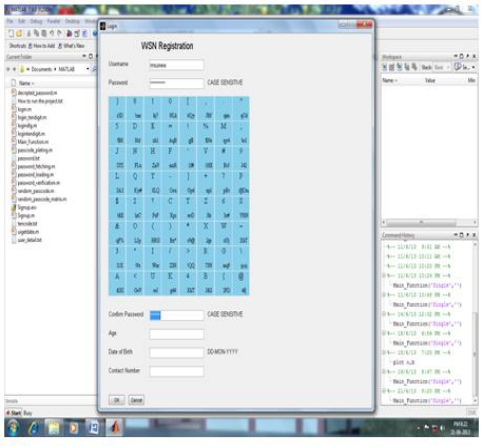


Figure-5.9. Second Level of Authentication: End userRegistration – Username and Password selection usingImage Patterns (Case Sensitive)and entry made by Random Numbers

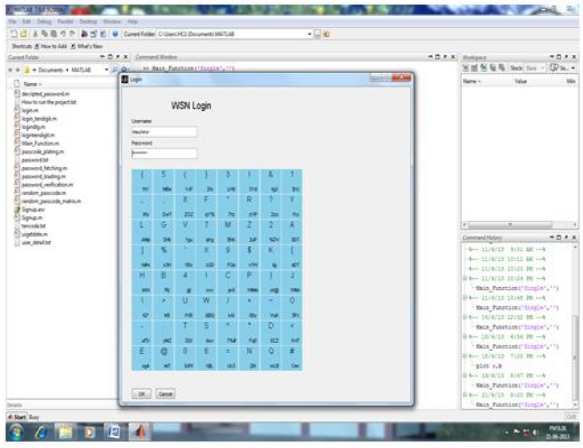


Figure-5.10. Second Level of Authentication: End user Login:Username and Password (Case Sensitive)

After finger-print authentication and image based authentication an end user gets authentic message from the server. Thus two level of authentication makes an end user not to leak any secret of information to the malicious users. This kind of system can be recommended to use in any confidential scenarios.

6. CONCLUSION

Broadly, constitute information security through authentication which is the focus of this paper for wireless sensor networks. After identification of sensor nodes in wireless sensor networks it is a compulsory action to procure information on it. There are generally two motives for taking this combined action:

- To improve usability and accuracy, combining items from different authenticating factors improves the accuracy of the authentication process. It may also lead to reduction in the false rejection rate of legitimate users.
- To improve the authentication process, integrity by reducing the effect of certain items in some factors that is prone to vulnerabilities that weaken it. The combining technique, therefore, reduces the risk of false negatives where, for example, impersonating users can succeed in accessing the system.

The discussion above provides one very important element of authentication, that different mechanisms provide different levels of authentication effectiveness. Choosing the most effective authentication, therefore, depends on the technology used and also on the degree of trust placed on that technology. To address these facts, an effective authentication scheme with dynamic mechanism is proposed. This authentication scheme is to be incorporated in sensor nodes in wireless sensor networks.

REFERENCES

[1] http://www.eetimes.com/document.asp?doc_id=1278992.

[2] Daniele Puccinelli and Martin Haenggi, "Wireless sensor networks: Application and challenges of ubiquitous sensing," Third Quarter 2005, IEEE Circuits And Systems Magazine,1531-636X/05/$20.00©2005, IEEE, 2005.

[3] W. Qinghua and B. Ilangko, "Wireless sensor networks – An introduction, dept. of electronics and telecommunications, Norwegian University of Science and Technology, Norway." Available: www.intechopen.com.

[4] K. Sanjay, D. Deepti, and K. Mahesh, "An efficient key distribution scheme for wireless sensor networks using polynomial based schemes," 2012 International Conference on Information and Network Technology (ICINT 2012), IPCSIT (2012) © (2012) IACSIT Press, Singapore. Available: sanjay_kumar@benpour.com, 2012.

[5] K. Damandeep and S. Parminder, "Various OSI layer attacks and countermeasure to enhance the performance of WSNs during wormhole attack," *Short Paper, ACEEE International Journal on Network Security*, vol. 5, 2014.

[6] A. K. Phiza, K. K. Patidar, S. Gajendra, and T. Mukesh, "False misbehavior removal in clonal selection mechanism based on watchdog by the use of transition point in a wireless sensor network," *Current Trends in Technology and Science, ISSN: 2279-0535, Issue: 4(June-July 2014)*, vol. 3, 2014.

[7] S. Vartika and S. Samjiv, "A review of existing security frameworks and encryption methods for wireless sensor networks," *International Journal of Innovations & Advancement in Computer Science, IJIACS, ISSN 2347-8616, Issue 2, April 2014*, vol. 3, 2014.

[8] P. C. Shahare and N. A. Chavan, "Secure and efficient sink node location privacy technique in WSN," *International Journal of Application or Innovation in Engineering & Management (IJAIEM), ISSN 2319 – 4847, Issue 3, March 2014. Available: www.ijaiem.org*,vol. 3, 2014.

[9] D. G. Murugaboopathi, V. Geta, V. Sujathabai, T. K. S. Rathish Babu, and S. Hariharasitaraman, "An analysis of threat's in wireless sensor networks," *International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277-128X, Issue 10, October 2012*, vol. 2, 2012.

BIBLIOGRAPHY

[1] Z. Junqi and V. Vijay, "A new security scheme for wireless sensor networks," Department of Computing. Sydney, Australia: Macquarie University. IEEE Communications Society, IEEE

GLOBECOM 2008 Proceedings, 978-1-4244-2324-8/08/$25.00 © 2008 IEEE, {Janson, vijay} @ics.mq.edu.au., 2008.

[2] F. L. Lewis, *Wireless sensor networks.* To Appear in Smart Environments: Technologies, Protocols and Applications. Ed. D. J. Cook and S. K. Das. New York: John Wiley. Associate Director for Research, Head, Advanced Controls, Sensors, and MEMS Group, Automation and Robotics Research Institute, The University of Texas at Arlington, 7300 Jack Newell Blvd. S, Ft. Worth, Texas. lewis@uta.edu. Available: http://arri.uta.edu/acs, 2004.

[3] E. Mohamed Hamdy, K. Muhammad Khurram, and A. Khaled, "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography," *978-1-4244-6734-1/10, © 2010 IEEE*, 2010.

[4] K. K. Takashina, S. Tsuruoka, and Y. Miyake, "Modified quadratic discriminant functions and the application to Chinese character recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 9, pp. 149-153, 1987.

[5] D. Wenliang, D. Jing, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," *IEEE Infocom 2004, 0-7803-8356-7/04 © 2004*, 2004.

[6] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY), "Specification," *IEEE Std. 802.11*, 1997.

[7] M. H. Zweig and G. Campbell, "Receiver operating characteristic (ROC) plots: A fundamental evaluation tool in clinical medicine," *Clinical Chemistry*, vol. 39:4, pp. 561-577, 1993.