SAKGP: Secure Authentication Key Generation Protocol in WLAN

Latha P.H
Research Scholar
Visvesvaraya Technological University
Belgaum, India

Vasantha R, Ph.D
Prof.: Dept. of Information Science and Engineering
Sambhram Institute of Technology
Bangalore, India

ABSTRACT
Wireless LAN is one of the cost effective way to establish local networking as compared to wired network. Although the last decade has seen various sophisticated WLAN routers and devices, but few of them are actually found to be highly resilient against potential attacks on WLAN. Literatures also share evidence that such issues are yet unsolved and call for a serious modeling of issues and testing the security efficiencies. The prime reason behind this is the incapability of the existing security protocols to ensure reliable authentication system. Hence, this study presents a technique that uses the most recent versions of cryptographic hash functions to ensure the bidirectional authentication between the nodes and WLAN router. Finally, the paper discusses about mathematical modeling of the presented security protocol as well as accomplished results are compared with the existing system.

Keywords-component
Wireless LAN, Cryptographic Hash Security, Authentication, IEEE 802.11

1. INTRODUCTION
Wireless local area networks are commonly known as WLAN, is one of the cost effective manner of establishing networking in the local level [1]. As a replacement of the conventional wired line based networking system, WLAN is one of the hassle free medium of establishing communication channel. The applications of WLAN are already in use in various institution as well as the commercial enterprises. However, along with such advantageous features of WLAN, this typed of wireless networking is also encountering continuous security threats. Majority of the attacks that are applicable in normal wireless network are also applicable in WLAN, which makes the user much susceptible to various lethal attacks from the adversaries. Although, the producers of the wireless LAN routers incorporate higher degree of security protocols, but till date, none of the protocols are found to be robust or extensively secured. The common security protocols incorporated in the design principles of wireless routers are WEP, WPA, PSK, TKIP [2][3][4]. Various resources from authenticated research based literatures have furnished evidence about the security loopholes of such security protocols of WLAN [5]. The prime reason behind this security issues in WLAN is the absence of the physical connection between the wireless mobile device and the wireless routers. This phenomenon renders the system more vulnerable as it is near to impossible to identify if the wireless mobile computing device is basically connected to the regular/authorized wireless routes while performing communication. Hence, the media through which the nodes communicate has higher scope of compromise, which makes the user almost unknown about the facts. This fact also renders the wireless routes in WLAN lose its reliability from usage viewpoint.
Inspite of the potential support of productivity, handiness, and cost effectiveness in WLAN, it has been seen that the weak and unsecured communication channel is the root cause of various vulnerabilities. Some of the critical threats to the WLAN are spoofing, denial of service, and eavesdropping. The most frequently used security protocol like WEP is also not safe enough. WEP doesn't give enough sustainability from forgery attack and replay attack. Therefore, the area which we are dealing with in this paper is basically a novel idea about resisting the illegitimate entry into the wireless LAN. The threats to the wireless user in WLAN is increasing day by day and almost no commercially available solution exists that gives the full fledge security system over WLAN. The method for performing intrusion has mechanized to a large extent posing a greater challenge even for existing security protocols to perform surveillance against it. One of the biggest issues of WLAN system is its environment are easily prone for sniffing. Hence, we say that existing security protocols for performing authentication is never enough and there is a need of more robust security technique in WLAN. We felt that the design of the security systems should be done in such a way that i) it gives better dimensionality to authentication system, ii) it should be easy to use, iii) it shouldn't have time and space complexity, and iv) it should be almost difficult to crack in. Hence, keeping all the above significant anticipated factors in mind, we develop a solution which has all the above properties by the name Secured Authentication Key Generation Protocol (SAKGP) for permitting the existing WLAN system to have a multiple security checks for ensuring the most reliable authentication system. Section 2 discusses in brief about the prior research techniques found in literatures. Section 3 and 4 discuss about the problem statement of the proposed system followed by brief description of cryptographic hash function with special emphasis on evolution of SHA3 from its ancestral versions. Section 5 discusses about the mathematical modeling of SAK followed by elaborated discussion of the proposed system. Section 6 and Section 7discusses about the research methodology adopted in the study and implementation techniques respectively. Section 8 highlights the algorithm used in the study. Section 9 discusses about the performance analysis of the study, while Section 10 concludes the paper by summarizing the work.

2. RELATED WORK
The past decade has witnessed many solutions being offered in the literature that claims to be potential enough for providing security over WLAN. Each of the literature has their own architectures and policies; some are evaluated in real-time while some in simulated study. It was also seen that none of the literature has yet proved fruitful in mitigating the security breaches in Wireless Environment

till date. 802.11i standard for wireless local networks introduces WEP protocol to try to solve the problems of protection and to make the level of protection of wireless local networks similar to the protection level of wired local networks. However, some of the potential studies carried out in past to address the security issues of protocols in WLAN are briefly discussed here.

Mavridis et al. [6] have discussed and presented in detail an analytical procedure towards WEP and WPA2 cracking, derived from real-life situations. Haddadi et al [7] have proposed a hybrid wireless intrusion detection system (WIDS). To implement the WIDS, they designed a simple lightweight agent. The proposed agent detects the most destroying and serious attacks; Man-In-The-Middle and Denial-of-Service; with the minimum selected feature set. Odhiambo et al. [8] have demonstrated an integrated security model (ISM) that incorporates a drop policy to defend against DoS attacks. The outcome shows that their security model performs better to provide improved security in terms of confidentiality, integrity, authenticity and availability. Bittau et al. [9] have presented a novel vulnerability which allows an attacker to send arbitrary data on a WEP network after having eaves dropped a single data packet. Furthermore, they present techniques for real-time decryption of data packets, which may be used under common circumstances.

Liu et al. [10] have illustrated an overview of WPA / WPA2 vulnerabilities and current researches in the method of attacks in WPA/WPA2 are described. Sherman et al. [11] have developed for the UMBC Cyber Defense Lab cover a variety of important and timely IA topics. The author has performed vulnerability monitoring exercise in the real-time test bed and has received overwhelmingly positive reactions from students, who appreciated the practical, hands-on learning activities related to a useful and interesting topic. Jagetia and Kocak [12] have proposed a scrambling algorithm that reduces the vulnerability of the WEP. Both the software and hardware implementations of the algorithm reveal at least multifold improvement in security. Tsukaune et al. [13] presented a secure WEP operation against key recovery attacks. The method presented by the author requires at least 100,000 packets to recover the WEP key for attackers. Furthermore they theoretically evaluate their technique to operate a secure WEP communication.

Nobles and Horrocks [14] have focused upon flaws in the WEP encryption and authentication processes. There exist, however, vulnerabilities in the lower layers of the protocol stack that may be easily exploited to produce denial of service attacks. One area to exploit is the medium access control (MAC) protocol that aims to ensure availability and fair sharing of the available wireless bandwidth.

Omar et al. [15] have illustrated their work targets networks secured by the Wired Equivalent Privacy (WEP) protocol because of its widespread use and vulnerability to a multitude of security threats. By exploiting the existing ARQ protocol in the 802.11 standard, their proposed opportunistic secrecy scheme is shown to defend against all known passive WEP attacks.

From the literature, it can be visualized that WEP is the first protocol for data protection in wireless networks whose mechanism is designed to achieve three safety goals: authentication, confidentiality and message integrity. This mechanism is based on RC4 algorithm (an algorithm that can be trusted) but, still, WEP does not achieve safety goals completely. Basic WEP deficiencies come from unsafe authentication, repeated use and open transfer of IV, key management system and a mechanism for the protection of message integrity that is not applied properly. Although WEP protocol uses RC4 algorithm that is highly reliable, there are several safety deficiencies. All these deficiencies can lead to many threats to WEP safety goals.

3. PROBLEM STATEMENT

The problem statement of the proposed study is as follows:

"It is challenging aspect to design a framework in existing WLAN based server IEEE 802.11 standards for ensuring fail-proof and efficient user-authentication with robust key generation in vulnerable wireless environment."

Although there are abundant research publications done in past, as evident from previous section, for the purpose of enabling security in two factor authentication systems in past, but effectiveness of all these techniques are yet to be proved. A malicious event occurrence results in the cost of user system account. Even if the security of the individual user may be highest but the system may already be in risk. Majority of the research work carried out in the past has only focused on initial level of authentication. However, such schemes are not used after the user is successfully verified and accesses for the second time. Especially the studies carried out in [16] have stressed on the illegitimate attempt of intrusion in WLAN. We strongly believe that stressing on primary access level to create a potential security system cannot be reliable in long run as multiple malicious programs can eventually corrupt the security policy in future and successfully retrieves the user identity. None of the prior mentioned literatures have focused on escalating security privilege where the probabilities of malicious activities are always maximum and it initiates from normal access of any user. However, if such malicious event successfully incorporates within the system, the user will not be able to identify the root location of malicious program to perform quarantine.

4. CRYPTOGRAPHIC HASH FUNCTION

As the network is never secure where the hackers always attempt various malicious codes to find the alternative solution of cracking the encryption, a research question arises from the viewpoint of implementation as: Is secure hash algorithm can be considered as highly secured mechanism? This question is quite difficult to answer as there is an evidence where various researchers have discussed about the potential benefits of secured hash function in various authentication and authorization mechanism [17][18][19]. In order to do so, we need to have a more insight on various types of cryptographic hash functions [20]. In the area of cryptography, SHA-1, the most preferred one, is the initial version of hash function that generates 20 byte hash value [21]. The weakness of SHA-1 algorithm was explicitly discussed by RSA Conference in 2005 [22].

The next possibility directs on exercising on its revised version SHA-2, which was formulated on 2010. SHA-2 is designed to overcome the weakness of its previous version SHA-1 by offering some of the superior security incorporations. It is essential to understand that the study proposes a design for superior level of authentication and authorization without any scope of security loopholes. Moreover, our study also understands that user of such application may want to use it for banking transaction or some sort of sensitive communication which requires higher degree of privacy, confidentiality and non-repudiation. However, we don't find SHA-2 as a suitable algorithm for technically adopting in our study as we find that it is not that compatible in conventional operating system [23]. The next probability comes to the recent version called as SHA-3, which is recently formulated in 2012 by

NIST [24]. Interestingly, SHA-3, by its name, is not the revised version of SHA-2. However, NIST chose to introduce SHA-3 as a solution towards concrete evidences of attacks in SHA-0 and hypothetical attacks on SHA-1. SHA-3 deploys a class of algorithms that consider input as predetermined internal state of any size but generates a resultant bit stream of required size.

5. MATHEMATICAL MODELLING OF SAKGP

The proposed system considers designing the mathematical modeling of the secure authentication key generation protocol (SAKGP) in wireless LAN. Consider a set C that represents client side attributes of the WLAN system as exhibited by,

$$C = \{C_n | n = 8\} \quad (1)$$

In the above Eq.(1), C_n represents the *n* components considered for the proposed mathematical modeling. Adopting a G-based wireless router, the highest scope of the attribute is considered to be 8. However, it may change based on the versions of the wireless router deployed. For better experimental values on real-time statistics, we consider C_1 as Access point name, C_2 as access point IP address, C_3 as geographical location of the mobile computing device (laptop, Tablets etc), C_4 as MAC address of the mobile device, C_5 as system generated timestamp, C_6 as SSID name, C_7 as SSID authentication key, and C_8 bandwidth assigned. Similarly, the server attributes of WLAN can be highlighted as,

$$S = \{S_m | m = 3\} \quad (2)$$

In the above Eq.(2), S_m will represent the *m* components considered from server side, where S_1 represents Seed, S_2 and S_3 represents two different independent random functions. The system will then be designed for security encryption where the message blocks are subjected to logical operation for accomplishing the preliminary bits of the state. This state is then permuted invertibly. A state is designed for a specific array dimension of 64-bit word. The mathematical modeling considers finite internal state that considers bit stream of any user defined length and generates a desired length of bit stream. For the purpose of permuting message block, a size of the word is considered as

$$W_{size} = 2^{length} \quad (3)$$

In the above Eq.(3), the variable *length* is considered to be 6 in size as SHA3 uses 64 bits of word length. For designing a state, an array of (5 *x* 5 *x* w_{size}) bits is designed. Consider α[i][j][k] be considered as an input message bit of size (i *x* 5 + j) *x* w_{size} + k. It is assumed that α be deploying the tactics where the least significant byte is stored in the smallest address [25]. The index arithmetic is deployed with modulo 5 for the initial two dimensions and modulo w_{size} for the third dimension. Therefore, the permutation of the block is carried out in 12+2(length) iteration for the 5 sub-rounds as follows:

- The parity (*p*) is computed for each of the 5 *x* w_{size} for 5 bit column, and logical operation is applied on it for two adjacent columns in a regular pattern. Mathematically, it can be represented as

$$\alpha[i][j][k] \oplus = p(\alpha[i][j-1][k]) \oplus p(\alpha[i][j+1][k-1]) \quad (4)$$

- The next sub-round consists of performing a circular shift [26] of every 25 words using triangular number. For better preciseness, α[0][0] is never subjected to circular shift (0≤t<24), that leads to

$$\alpha[i][j][k] = \alpha[i][j][k-(t+1)(t+2)/2] \quad (5)$$

- The total of 25 word are permuted using a fixed pattern as follows:

$$\alpha[j][2i+3j] = a[i][j] \quad (6)$$

- The bitwise integrates alongside of the row as follows,

$$\alpha = \alpha \oplus (\neg b \,\&\, c) \quad (7)$$

The last step is the highly crucial step of SHA3, where in specific round *r*, for 0≤a<length, α[0][0][2^a-1] is XORed with (a+7r) bits of message that potential breaks the symmetry conserved in other sub-rounds. This is the prime reason why SHA3 is so strong and can be highly used in security formulation of WLAN.

The next step of the proposed mathematical formulation will be to generate a new seed (S_1) by integrating MAC and Timestamp as follows,

$$S_1 = \sum_{i=0}^{n} \sum_{j=0}^{t} (C_4 + C_5) \quad (8)$$

In the above Eq. (8), *i* and *j* represents the iterations for n components (where *n=8*) and individual time (t). The summation is done considering both *i* and *j* every time. The seed (S_1) is generated by considering both MAC address of user's mobile device (C_4) and timestamp (C_5), which is then subjected to SHA3 encryption mechanism as follows,

$$f(x) = SHA3(S_1).S_2 \quad (9)$$

Consider f(x) is just a function that stores the encrypted value of S_1 after performing SHA3 and S_2 is an independent random function. For better robustness, the system performs encryption for the second time as,

$$g(x) = f(x).S_3 \quad (10)$$

The Eq.(10) is basically adapted over deploying MD5 algorithm for S_3, where S_3 is an independent random function. An interesting part of this mathematical formulation is the usage of S_2 and S_3 attributes. It is designed in such a manner that using above mathematical strategies, it gives triple advantages i) it implements dual level of secure authentication protocol. The first level of authentication is made when the Client (C_n) attributes are fed to the WLAN server attributes (S_m) to generate first authentication key, S_2 and S_3 attributes. The second level of the authentication consists of when the client enters currently generated first authentication key, S_2 and S_3 attributes. In this case, it is to be noted that WLAN server doesn't share the key and only share the S_2 and S_3 attributes with the clients. Hence, the two keys are matched for final authentication key generation. ii) due to application of SH3 and MD5 in two different steps and the two attributes S_2 and S_3 are not dependent on each other, likelihood of performing cryptanalysis on the system is extremely less, iii) the generated key is very small in size and doesn't store in network or in WLAN server and hence its time and space complexity O (*n* log *n*) is very small making the system more cost effective with higher degree of security.

6. PROPOSED SYSTEM

The proposed SAKGP discusses about the significant encryption technique that play a critical role in the implementation of the security of WLAN. All the possible inputs and output variables for designing the algorithm is done and then objectives of the study

are re-visualized to formulate the algorithms for user registration, hash function implementation, and proposed secure authentication key generation on IEEE 802.11 interface. In this stage, the initial secure authentication key is designed to generate in both WLAN server sides as well as in user side (Fig.1). A user interface is designed where user will register themselves with the WLAN server. The tools used for this purpose will be JDK, JSP, Apache Tomcat as software and hardware will consist of standards 32 bit Windows OS with Windows XP and minimum 1 GB Ram and 1.84 GHz processor speed. For the secure authentication key generation, the hardware profile consist two hash functions (SHA-3 and MD5), MAC address and timestamp. The independent random function is represented as (S_2, S_3). SHA3 and MD5 are used as standard algorithm. However, the proposed system doesn't deploy any conventional encryption or decryption technique. The proposed system considers the digital signature of the data (seed) and digital signature will be authenticated or matched on WLAN server side as well as on client side. It should be noted that digital signature does not carry any information about the data however it is just an identification of the data but the cipher text of the data contains the original data in interchanged format. This will mean that intrusion on digital signature does not yield data. However, there is a fair feasibility of data retrieval from cipher text.

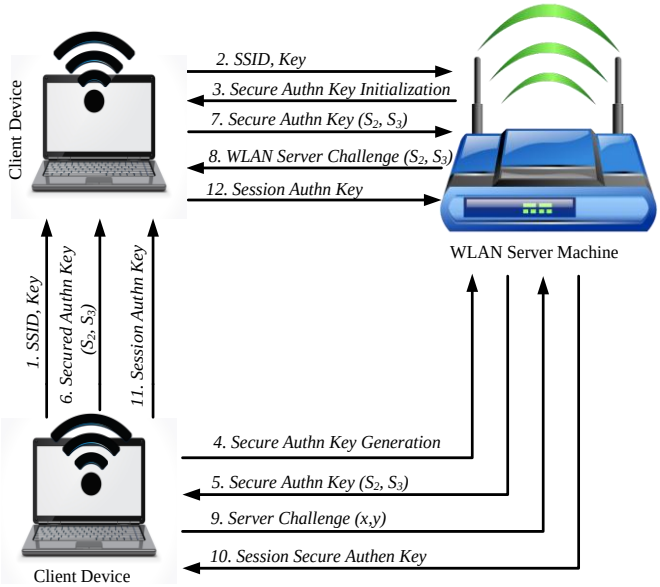

Figure 1 Schematic Diagram of SAKGP

Hence, we chose not to perform encryption and decryption technique directly. It generates the values of S_2 and S_3 (independent random functions) where 'S_2' is number of iterations for SHA-3 and 'S_3' is number of iterations for MD5. After processing, it results in 128-bit keys of MD5 but it will require to manually feed the secure authentication key. However, secure authentication key systems are designed in such a way that it gives privilege to enter manually and not automated. It is computationally complex process for feeding the 128 bit data as it gives rise to error prone processes. Hence, it is to be converted into byte-to-word format by using alternative dictionary encoding. For that, the 128-bit collapses it to 64-bit result, which is further decomposed to pairs of bits that are summed together. The 2 least significant bits of this sum are encoded in the last 2 bits of the 6 word sequence with the least significant bit of the sum as the end bit encoded. All the complaint servers should be in agreement with the 6 word input that deploys the standard dictionary. The authorization enclosed by a 64-bit key could be enclosed by six words from the standard dictionary with space present over for parity and that six words will be long enough for security and short enough for user-friendly. Authentication will draw closer on action as a security purpose for the initial (static) password. User will login with initial (static) password and initial authentication key is generated during registration phase. The initial (static) authentication key will be checked for validity. Then the WLAN server will request for secure authentication key. The user will generate secure authentication key by using their IEEE 802.11 interface and reply back to the WLAN server.

However, it is the biggest challenge for the WLAN server that they should generate same secure authentication key for authentication purpose. The WLAN server will check the generated secure authentication key by using S_2 and S_3 attributes entered by user as mentioned in the above step. Once the WLAN server is authenticated, the WLAN server will generate the secure authentication key by using user-seed and new random generated S_2 and S_3 attributes. The WLAN server will send the challenge to the user by sending S2/S3 attributes only. Based on the above challenge, the user must be able to generate an authentication key, and the generated secure authentication key will be checked on the WLAN server side. If both the authentication keys match, then it is said to be authenticated and can access the application. It can be seen from the above operation that we are introducing a novel concept of authentication. Majority of the work conducted in literature survey considering secure authentication key has focused on user authentication only, however, in order to ensure better security, the contribution of the proposed work is introduce a novelty by utilizing the concept that neither user nor WLAN server can be blindly trusted to each other. Therefore, we introduce the novelty in mathematical modelling of SAKGP by considering an initial step where user will be given a chance to verify the authenticity of their WLAN server and if scored success in this authentication, then WLAN server will be given chance to authenticate user. Authorization steps follow only after successful authentication from both the parties.

7. RESEARCH METHODOLOGY

The proposed system presents a secure authentication system that is built over the enhancement work carried out over the top of dual authentication protocol discussed by Zheng et al. [27]. Keeping the robustness of user authentication as well as authorization system, the proposed system introduces multiple layer of security mechanism in most simple and yet effective manner that uses considerably less authentication as well as authorization time. Thereby the proposed system posses the charecteristics of privacy, confidentiality, and non-repudiation of the security services to the user. The study encapsulates the development of an Application for the IEEE 802.11 standards for secure authentication key generation and creation, including all fundamentals that are necessary to do this. Secure authentication key generations are implemented keeping majority of the WLAN application in mind.

The present work is compared with the work carried out by Zheng et al [27], hence, it is critical to understand the uniqueness and novelty in the approach of our technique. One of the notable enhancement works that has been carried out was to ensure much higher level of security incorporation. The study conducted by Zheng et al [27] discusses about the usage of the hash function using SHA-1, which is definitely not secured algorithms in cryptography presently. SHA-1 has various issues when it is

implemented on public network for which purpose SHA-1 should not be preferred (or should be amended) algorithm for any researcher when the experiments need to be carried out in large public network with higher level of untraced intrusion activities. Hence, the proposed study considers adopting SHA-3 instead of conventional and error-prone SHA-1 algorithm. One of the prime reasons behind this is SHA-3 uses different patterns of design architecture compared to SHA-1 for which reason, common attacks applicable over SHA-1 will never work on SHA-3. Zheng et al. [27] has used single hash function for first time secure authentication key generation, whereas we choose to integrate two different hash functions in two different directions (S_2 and S_3) at every time in secure authentication key generation. Adopting this second technique of enhancement will yield secure authentication key generation that is potentially strong compared to Zheng et al [27] approach. The third enhancement is towards the length of the secure authentication key generation generated. While working on cryptographic algorithm, emphasizing on key management is the most prominent phase of the design work. Therefore, in this regard, exploring the work of Zheng et al [27] was found to use length (128 bits) key size which is not at all a user friendly approach. The existing study by Zheng et al. [27] may be better guideline for our study by discussing the approach of implementing a security protocol, but however, it was never user friendly. The term 'user friendly' will mean that the generated authentication key is large enough which cannot be memorized as well as it sufficiently occupies memory and hence it is complex process. Since the numeric format of secure authentication key generation was found very complex and error-prone, we choose to enhance this third technique by using byte-to-word conversion with alternate dictionary encoding for the secure authentication key generation. This makes the secure authentication key generation robust enough for security and short enough for the user. The proposed study attempts to minimize the operational cost by generating the authentication & authorization components on mobile devices connected in WLAN. However, Zheng et al [27] also did the same thing. It should be noted that Zheng et al. [27] took assistance of remote communication design in WLAN. We criticize this approach with a fact that proliferation of various mobile devices like Smartphones and Tablets are on rise and similarly there is a rise of security threats as such smartphones gives better internet access while on the move. All the mobile devices (laptop, PDA, smartphones, Tablets etc) however have mobile operating system which assists in evaluation. Hence, security considering such mobile device was never a part of discussion of existing system, which we choose to enhance it. Therefore, because of generation of efficient authentication and authorization using present work, the system is designed further more secure because it is not accessible to other networks as well as among two different users on same WLAN. The proposed system is designed on windows using Java as programming tool.

8. IMPLEMENTATION

The proposed SAKGP is formulated and developed using Java as it is one of the most preferred tools for designing a framework of network and security. The proposed system is basically under the domain of network and security where it is considered that whenever a data packet travels through any public networking system, it is highly prone to various types of intrusions usually generated by illegitimate members existing latently in the network [28]. It is already known that the design of socket mechanism in java is quite well adopted in majority of the application that demands security when the application runs on large network called internet. The java package also provides various APIs and framework [29] that includes potential functionality like securing the ongoing communication, incorporating integrity on the message under transmission, and definitely encrypting data packets. Hence, the proposed study adopts using Java 2 Standard Edition that has rich collection of API, which provides enhanced security and encryption platform using some of the potential java packages e.g. java.net and java.security [30].

This section exhibits the Algorithm that is originally deployed for designing the proposed cryptographic hash function. The class basically converts all the bytes to the hexadecimal format. The algorithm basically uses SHA3 that operates on 1024 bit of message block and 512 bit of intermediate hash value. The algorithm is basically mapped as 512-bit of block encryption standard that performs ciphering on the intermediate hash value with an assistance of message block as the key. Finally, the newly generated secured authentication key using SHA3 is generated from the server side and reaches the IEEE 802.11 interface of the user. The new user considers this hash value for getting the final secured authentication key.

Algorithm: New Secured Hash Algorithm
Input: C and S attributes
Output: Secured Authentication Key
START
1. Define a class of Secure Hash Algorithm
2. Define a static class for byte to hexadecimal conversion
3. char hexDigit[] = {'0', '1', '2', '3', '4', '5', '6', '7', '8', '9', 'A', 'B', 'C', 'D', 'E', 'F'};
4. String Secured authen key=null;
5. String MAC_Address=C_4;
6. String Timestamp=C_5;
7. Final seed=C_4+C_5;
8. Create String Buffer;
9. For (j=0; j<b. *length*; j++)
10. Append (hexDigit[(b[j] >> 4)]);
11. Append(hexDigit[b[j] & 0x0f]);
12. Create class for SHA3.
13. MessageDigest = get Instance of ("SHA-512");
14. Update(getBytes());
15. Byte_output = md_digest();
16. srt=bytes_To_Hexadecimal(output);
17. String seed=new String();
18. seed="abc";
19. String result=null;
20. result=seed;
21. for(int i=0;i<5;i++)
22. if(i==0)
23. for(int j=0;j<2;j++)
24. result=SHA3 (result);
25. Print Secured Authentication key

The proposed algorithm considers the hardware profile (MAC Address and Timestamp) of user's machine as an input for generating the initial secured authentication key. Seed information plays one of the critical roles in the program. The algorithm uses SHA3 and MD5 on the seed information and successfully generates the ultimate secured authentication key as well as server challenges, which will be mandatorily required by the user to perform the final step of authentication system proposed in the current study. The application is designed with two modules e.g. i)

Authentication from Server side and ii) Authentication from client side. The proposed system is basically a framework that is tested on a transactional application considering financial institution as a case study where the user is required to be efficiently authenticated and thereby authorized. The proposed application evaluated on Windows platform has higher interoperability, although the application may support both in windows and Linux, but in reality, it is supported in Linux platform.

9. PERFORMANCE ANALYSIS

The primary usage of the proposed system is that it can be utilized for an efficient identification of a legitimate member for having an access rights in their account in WLAN. As the entire framework is based on the enhanced operation of secure authentication key generation as well as updated cryptographic hash function (SHA3 and MD5) without storing the authentication token. Hence the proposed system is highly expected to excel some of its best security measures. It should be also known that although there are abundant micro stages of implementation of the proposed system, the fundamental concept of the proposed framework basically uses the IEEE 802.11 standards as a medium to perform authentication procedure of the proposed study. However, underlying concepts of SHA3 and MD5 makes all the differences in the security incorporations that make the authentication more robust as compared to the standard techniques adopted by Zheng et al. [27]. Therefore, this section will discuss the performance analysis of the proposed system with the work of Zheng et al. [27] using following parameters for the comparative performance evaluation. The detailed information of the adopted tools are as below in table 1

Table 1 Software / Hardware Requirement Specification

SL #	Softwares Used	Hardware Used
1	Operating System: Windows XP (on x86-32 and x86-64), Android OS	Processor: 2GHz CPU
2	IDE: Eclipse 3.5	Memory: 1 GB RAM
3	Software Package: JDK 1.6, 1.7	Hard disk: 20 GB(minimum)
4	Software Technologies: JSP, Android	Trusted Handheld Device: Android mobile phone with 832 MHz processor and minimum 1GB Micro SD, 1200mAh battery
5	Browser: Firefox 15.0.1, Google Chrome, Internet Explorer 7 and above	
6	Programming Language: Core-Java/J2EE	
7	Web Server: Apache Tomcat 5.5	
8	Database: MYSQL	

In order to perform simulation of this phase, the proposed system has adopted the usual mitigation technique using secured hash algorithm. The proposed work considers a node as an important asset which is subjected for DDoS for evaluation. For the purpose of comparative analysis, the proposed system is compared with the Zheng et al [27] study. The results were mainly studied with respect to energy being consumed by the nodes which performing computing and amount of data being transferred during complete data transmission process in WLAN.

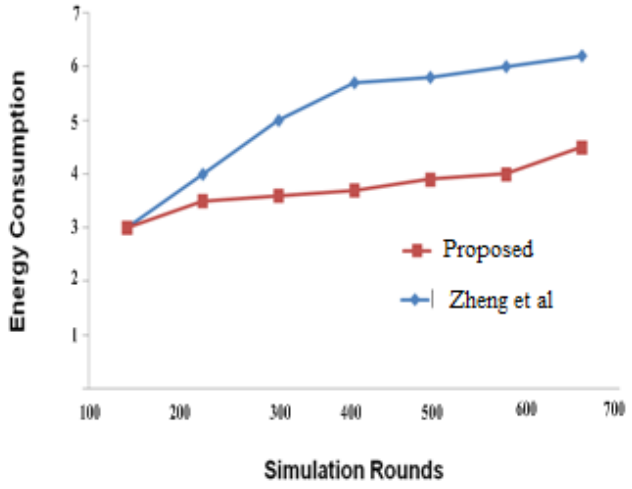

Figure 2 Outcome for energy consumption

Fig.2 represents the outcome of the study with respect to the amount of energy consumption for the computing nodes. It can be seen that the proposed technique was found to show quite uniformity even in the power consumption. The result shows that the power consumption is quite linear between the simulation rounds of 200-400 and again between 500-600 compared to existing system. Although there were extensive usages of the energy in the initial round between 100-200 rounds of the proposed system, however, when data transmission is performed using the proposed technique, the node seems not to consume the energy in increasing manner. The outcome is quite significant from that of the study performed by Zheng et al. [27].

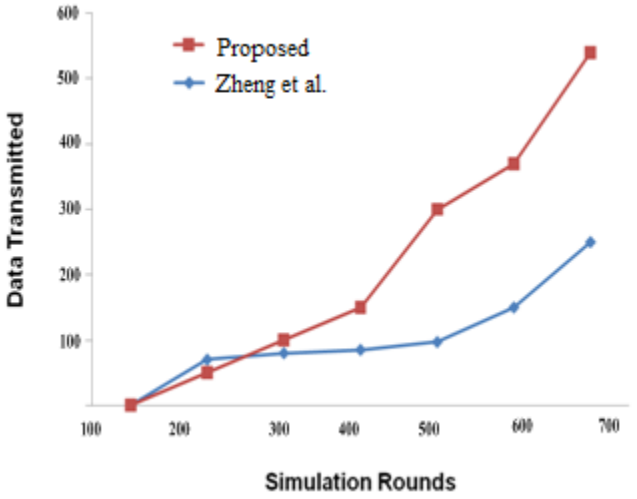

Figure 3 Outcome of WLAN Data Transmission

Fig.3 exhibits the outcome where it can be seen that with the increase of simulation rounds from 100-700, the quantity of data transferred is proportionately increased. This facts highlights the robustness of the system, where data (in bytes) were tested from 0-600 bytes transmittance using proposed protocol. Hence, due to efficient decision making charecteristics of proposed system using Secured Hash Algorithm for establishing a secured route, it is

possible to transmit increasing load of data packets even in congested traffic of WLAN

Processing Time: An effective time required to process the complete proposed algorithm for performing the user authentication system is termed as 'processing time' in our performance analysis. We assume that effectiveness of the proposed algorithm against mitigating any types of attack/intrusion from illegitimate member and an effective processing time required to perform the procedure as the attribute of performance analysis. In order to carry out the analysis of processing time, we chose to use Apache Tomcat as web server, where the proposed application resides. A simple LAN and WLAN network is considered to carry out the evaluation considering 40 numbers of users, whose authentication will require to be evaluated. Also, the 40 different numbers of the user uses WLAN to cross check the authentication process. Figure 4 shows the final results accomplished while evaluating the proposed system processing time with Zheng et al [27] model.

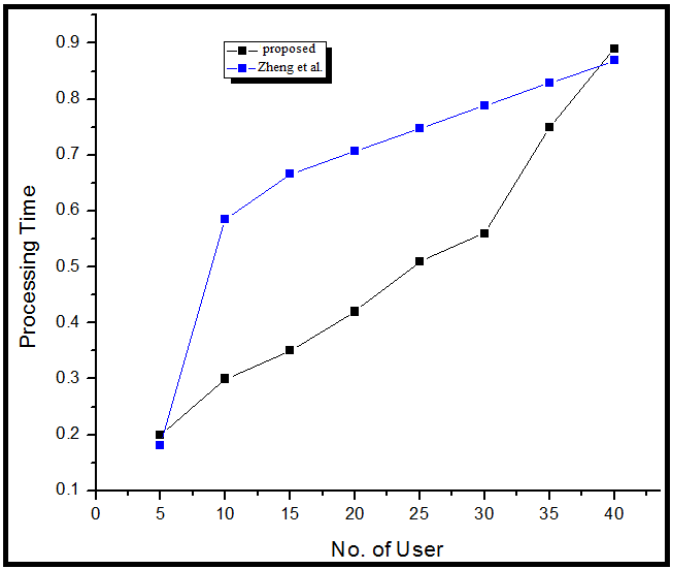

Figure 4 Total Processing Time

It can be seen that proposed system takes considerable less time as compared to Zheng et al. [27] model that used SHA1 hash function that is usually deployed for performing computation on a compact depiction of a message. However, proposed approach using SHA3 will need extra time to produce a message digest in comparison to its previous version of SHA used by Zheng et al. [27]. The prime reason behind this is that message digest generated by SHA-1 is bigger as compared to that of SHA3. However, SHA3 will have extra bit blocks in the elementary function that improves the encryption mechanism exponentially compared to SHA-1. Hence, the proposed SHA3 along with MD5 implementation is found potentially stronger compared to Zheng et al. [27] approach.

The results also show that client can access the privilege account in faster track proving its compatibility in mobile devices too. The term 'priviledge account' will mean resources that are meant to be accessed by only legitimate user. The performance of the system is tested by installing the framework in different types of mobile devices, which shows no significant changes in the service delivery. Hence, it can be said that an optimal performance which is user-friendly and highly secure is recorded in this evaluation process. The performance of the proposed algorithm can be stated as better and highly secure as it has two inherent characteristics: i) The processing speed is highly faster ii) using SHA3, it is almost impossible to explore the message mapping with the pre-determined hash function. iii) Enhancing the cryptographic hash function into two directional property incorporates more security in the encryption process as well as faster access time is accomplished as server can generate challenge and can authenticate it is faster process, thereby proving a strong way to mitigate hash function collision.

Security Analysis: The proposed evaluation of security analysis lies in the efficient operation of the security functionality for performing secure transaction for the considered application on financial institution. Review of literature has depicted various application of cryptographic hash function for performing authentication process, which was always found less stable and less resiliency to various types of lethal attacks over internet or large corporate network. While reviewing the work proposed by Zheng et al. [27], it was found that SHA-1 can be potential security algorithm for mechanizing robust authentication system. However, it is not true as SHA-1 is also explored with multiple security incapability and reported attack evidences found in history. Therefore, the implementation has been carried out using SHA3. SHA3 was designed to mitigate the security loopholes that SHA-0 or SHA-1 couldn't afford to furnish in secure and efficient authentication mechanism. One of the attribute for comparative analysis can be the sizes of the hash codes where present work incorporates SHA3 always excels better than conventional SHA-1. Performing evaluation at a micro-level for the proposed study found that SHA-256 is somewhat time-consuming pertaining to the processing of the secure key or the server generated challenges while multiple networks are considered as a media to transmit the final authentication token. The proposed system adopts the usage of SHA3 which is considerably faster compared to the conventional SHA-1 adopted by Zheng et al. [27]. After performing the experiments in both 32 bit as well as 64 bit machines with windows operating system and standard core i3 processors, it was found that proposed framework using SHA3 performs faster generation of challenge, seed, and coordinates as compared to SHA-1 implementation studied from Zheng et al. [27] contribution. The prime reason behind this fact is that SHA3 performs 80 rounds of operation on 128 bytes blocks while SHA-1 is performed for 20 bytes of blocks. Experimented on 40 machines of 64 bit, the results accomplished shows significant level of security with less computational time compared to SHA1. However, when a question of cost efficiency is raised, it can be said that SHA3 may be quite expensive in nature exclusively in constrained machine configuration. But, it will not be a problem of any concern as the proposed framework chooses not to store any hash value or have any features of reusability of hash codes.

10. CONCLUSION

This paper has discussed about the cumulative analysis of the results that have been accomplished from the proposed study. This paper also discusses the outcome with respect to performance analysis and with respect to security analysis. Compared with the base technique adopted in the past in securing WLAN, the proposed system offers better security schemes in much cost effective manner to ensure optimal performance with respect to authentication mechanism. The proposed framework is developed and experimented on IEEE 802.11 interface which is increasingly accepted by corporate and various institutions. Hence, technical adoptability of the proposed framework can be highly ensured. From the performance viewpoint with respect to security, the proposed framework design is highly resilient to dictionary attack,

spoofing attack, internet spamming and any sorts of unauthorized access due to its multiple layer of security that is highly impossible to imitate or accessed by attacker. Neither the proposed scheme does require any extra hardware token to be carried by user as mobile phone is used as an authentication token. As the proposed system do not use any sorts of complex cryptography, so it ensures an optimal verification as well as authentication time that was reflected as major trade-off in previous work. Therefore, it highly guarantees large scope of future enhancement by developer for much better security prospects in their problems.

11. REFERENCES

[1] http://www.gsmarena.com/glossary.php3?term=wi-fi

[2] A.E.Earle, "Wireless Security Handbook," Auerbach Publications, pp.348, 2005

[3] "National Institute of Standards and Technology NIST 800-97", retrieved from Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

[4] B.Mitchell, "WPA - Wi-Fi Protected Access An Article from Computing", Wireless/networking. Retreived from http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm, 2004

[5] Latha.P H, Vasantha R, Review of Existing Security Protocols Techniques and their Performance Analysis in WLAN, International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS), Vol.7, pp. 162-171, December 2013

[6] I.P.Mavridis, A-I.E.Androulakis, A.B.Halkias, P.Mylonas, "Real-Life Paradigms of Wireless Network Security Attacks," Informatics (PCI), 2011 15th Panhellenic Conference, pp.112-116, 2011

[7] F.Haddadi, M.A.Sarram, "Wireless Intrusion Detection System Using a Lightweight Agent," Computer and Network Technology (ICCNT), 2010 Second International Conference, pp.84-87, 2010

[8] O.N.Odhiambo, E. Biermann, G.Noel, "An integrated security model for WLAN," AFRICON, 2009. AFRICON '09. Pp.1-6, 2009

[9] A.Bittau, M.Handley, J.Lackey, "The final nail in WEP's coffin," Security and Privacy, 2006 IEEE Symposium, pp.15-400, 2006

[10] Y.Liu, Z.Jin, Y.Wang, "Survey on Security Scheme and Attacking Methods of WPA/WPA2," Wireless Communications Networking and Mobile Computing (WiCOM), 6th International Conference, pp.1-4, 2010

[11] A.T.Sherman, B.O.Roberts, W.E.Byrd, M.R.Baker, J.Simmons"Developing and delivering hands-on information assurance exercises: experiences with the cyber defense lab at UMBC," Information Assurance Workshop, Proceedings from the Fifth Annual IEEE SMC , pp.242-249, 2004

[12] M.Jagetia, T.Kocak, "A novel scrambling algorithm for a robust WEP implementation [wired equivalent privacy protocol," Vehicular Technology Conference, IEEE 59th , vol.5, pp.2487-2491, 2004

[13] T.Tsukaune, Y.Todo, M.Morii, "Proposal of a Secure WEP Operation against Existing Key Recovery Attacks and its Evaluation," Information Security (Asia JCIS), Seventh Asia Joint Conference, pp.25-30, 2012

[14] N.Phil, A.P. Horrocks. "Vulnerability of IEEE802. 11 WLANs to MAC layer DoS attacks." pp. 14-14, 2004

[15] Y.Omar, M.Youssef, E.H. Gamal,"ARQ secrecy: From theory to practice," Information Theory Workshop, ITW. IEEE, pp.6-10, 2009

[16] S. A. Pattar, Detection Of Rogue Access Points Present In The Wlan At The Server Side, Proceedings of IRF International Conference, 2014

[17] S.Q. Wang, J.Y. Wang, Y.Z. Li, "The Web Security Password Authentication based the Single-Block Hash Function", Elsevier, 2013

[18] Z-Y Wu, Y. Chung, F. Lai, T-S Chen, and H-C Lee, "An Enhanced Password-Based User Authentication Scheme For Grid Computing, An Enhanced Password-Based User Authentication Scheme For Grid Computing", Volume 7, Number 7(A), pp. 3751-3760, 2011

[19] C. K. Kumar, C. Suyambulingom, "Multicollisions and iterated Cryptography hash functions", Journal of Computing Technologies Vol 2, Issue 3 ISSN 2278 – 3814, 2013

[20] H. Delfs, H. Knebl, "Introduction to Cryptography: Principles and Applications", Springer, Computers, 367 pages, 2007

[21] H.F. Tipton, M. Krause, "Information Security Management Handbook", Fifth Edition, CRC Press, Computers, 2036 pages, 2004.

[22] http://www.emc.com/emc-plus/rsa-labs/historical/hash-function-update-potential-weakness-in-sha1.htm

[23] http://www.entrust.net/knowledge-base/technote.cfm?tn=8526

[24] http://keccak.noekeon.org/

[25] http://www.cs.umd.edu/class/sum2003/cmsc311/Notes/Data/endian.html

[26] http://en.wikipedia.org/wiki/Circular_shift

[27] X. Zheng, C. Chen, C-T Huang, A Dual Authentication Protocol for IEEE 802.11 Wireless LANs, pp.565-569, IEEE, 2005

[28] B. A. Kumar, K. Kavuri, "Novel approach for preventing hackers in data communication", International Journal of Computer Science and Advanced Computing, Vol.1, Iss.1, April. 2013

[29] J. Friesen, "Learn Java for Android Development", A press, Computers, 806 pages, 2013

[30] N. Nagaratnam, L. Koved, A. Nadalin, "Enterprise Java Security: Building Secure J2EE Applications", Addison-Wesley Professional, Computers, 581 pages, 2004

12. AUTHOR'S PROFILE

Dr. R. Vasantha is presently working as Professor in Sambhram Institute of Technology, Department of Information Science and Technology, Bangalore. After completion of Ph.D from Indian Institute of Science (Bangalore), she has accomplished potential 14 years of experience working as research associate in University of New South Wales (Sydney), University of East Anglia (England), Indian Institute of Science (Bangalore). Her research interest includes Applied Mathematics, Network Security, Data mining, Finite Automata and Formal Languages, Cryptography, Compiler Design, Image processing, Pattern recognition, Algorithms, Graph Theory, and teaching in applied mathematics, Computer Science subjects.

Latha P.H. is currently working as a Assistant Professor at Atria Institute of Technology in Dept of Information Science, Bangalore,. She has total of 15 years of experience in teaching field. After completion of graduation from B.M.S College of Engineering in Information Technology, she has completed her Master's of Science in Information Technology from KSOU Mysore and Masters of Technology in Computer Network Engineering at A.M.C College of Engineering, Bangalore. Currently she is an research scholar at Visveswaraya Technological University, Belguam, India. Her research interest includes security in networks.