International Journal of Electrical and Computer Engineering (IJECE)
Vol. 5, No. 4, August 2015, pp. 859~868
ISSN: 2088-8708

MDS-WLAN: Maximal Data Security in WLAN for Resisting Potential Threats

Latha P.H. *, Vasantha R ****
*Department of Information Science & Engg., Atria Institute of Technology, Bangalore, India
** Department of Information Science & Engg., Sambhram Institute of Technology, Bangalore, India

Article Info

Article history:

Received Jan 23, 2015
Revised May 5, 2015
Accepted May 28, 2015

Keywords:

Cryptography
Data Security
Key Management
Security Protocol
WLAN

ABSTRACT

The utmost security standards over Wireless Local Area Network (WLAN) are still an unsolved answer in research community as well as among the commercial users. There are various prior attempts in proposing security of WLAN that lacks focus on access point and is found to be quite complex implementation of cryptography. The proposed paper presents a novel, simple, and yet robust technique called as MDS-WLAN i.e. maximal data security in WLAN. The system is evaluated over laboratory prototype and mitigation measures are drawn for resisting wormhole attack, Sybil attack, and rogue access point issue in WLAN. The outcome of the MDS is compared with conventional AES and SHA that shows optimal communication performance and highest data security.

Corresponding Author:

Latha P. H.,
Asst. Prof: Dept of Information Science & Engg.
Atria Institute of Technology
Bangalore, India
E-Mail: researchvtulatha@gmail.com

1. INTRODUCTION

A wireless local area network (WLAN) is a distribution process for two or more devices that utilize high frequency radio waves and frequently incorporate a right to gain access point to the Internet. The applications of WLAN ranges from home to large scale networking. It allows the users to access internet using the access point (or routers), which can be also set up in adhoc manner. However, owing to the data communication in wireless medium, it also invites various vulnerable security conditions that affects the privacy of the users and renders the resources prone for various malicious attacks. At present, security protocols like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and 802.11i (WPA2) are used. However, WEP is a weak security standard [1] as the secret key it uses can frequently be splitted shortly with a fundamental Smart phone using available software tools. WEP is also an old IEEE 802.11 standard, which is outdated through WPA. WPA was a speedy option to enhance security over WEP. Wireless networks are more defenseless to attacks due to their imparted physical medium, open transmission of radio frequencies. The attacks on WLAN networks can be deliberate based on the two phenomena attacks on access point and attacks lying on their protocol stack. The fundamental issues that have been faced by the WLAN are security and signal interference. The issue with security can never be tackled completely however it can be minimized. To reinforce the security of devices, it is important to comprehend the security holes. For example, i) equipment have security settings disable through defaulting, ii) insignificant security is effectively broken, and iii).rogue access points are not difficult to send and hard to identify [2]. Apart from the security issues, another significant issue is awareness of security protocols among the users. Sometimes inspite of potential security protocols, the ignorance of users calls for creating a potential security breach in the network esbtablished by the routers [3]. Till now, numerous remote security protocols have been

composed and executed, however none turned out to persuade with the security threats that come consistently with new threats to our systems and information. Usually WLAN is used in providing wireless hot spots in large campus, hence it is quite feasible that various type of illegitimate member could also attempt to have an access to the router. The attacks may device various intrusive principle to perform intrusion in the WLAN routers and once routers are compromised, the other clients connected to the routers are equally prone to malicious programmes. The existing security protocols e.g. WPA and WEP are not at all secured against various attacks like Denial of Service, wormhole attack, sybil attack, sinkhole attack, routing attack, and rogue access point. Hence, mitigating all the attacks in a single algorithm is near impossible task.

Hence, this paper presents a very potential technique in terms of algorithms that aims to mitigate the lethal threats over WLAN. The prime contributions of this paper are as follows e.g. i) To present a technique to incorporate highest level of security on heterogenous WLAN routers, ii) To present a unique key management techniques that is inaccessible to even users as well as routers in worst scenario of node compromization, iii) To present a novel algorithm for node activation by the access points, iv) To present a novel algorithm for maximal data security for thwarting lethal attacks on WLAN, iii) To carry out real-time experiment and prepare a laboratory prototype on multiple machines and multiple varieties of routers and check for security efficiency. Sub-section 1.1 of Introduction discusses the background of the study where the prior research contribution has been discussed. Introduction sub-section 1.2 enlists the identified problems of the proposed study followed by discussion of proposed system in sub-section 1.3. Research methodology is discussed in Section 2, while sub-section 2.1 highlights about the test-bed scenario of the proposed study, Sub-section 2.2 discusses about the first algorithm while sub-section 2.3 discusses about the second algoritm. Section 3 discusses about the outcomes of the study, while concluding remarks are in Section 4.

1.1 Background

This section discusses about the background literatures of the study, where prior research implementation towards security threats in WLAN was found to be addressed. Kambourakis et al.[7] concentrate on quality declarations, which are of real vitality for client authorization They stress on the vital public key framework which obliges least changes in 3G center system components and signaling and give a rundown of the potential threats, which can be recognized in an apparent sending. Their trial assessment of the execution of two option test bed scenarios, demonstrates that computerized authentications technology is not just possible to actualize in present and future heterogeneous mobile systems. Balachandran et al.[8] observed that the mobile computing scene has changed both regarding number and kind of hotspot venues. There are a few innovative and arrangement difficulties staying before hotspots that can turn into a universal framework. These difficulties incorporate as verification, security, scope, administration, area administrations, charging, and interoperability. Mohanty et al. [9] proposed a novel 3G/WLAN coordinated building design utilizing the outsider, Network Inter-working Agent (NIA), to coordinate 3G and WLANS of diverse suppliers. This building design does not necessitate the presence of immediate SLAS among the system suppliers. Subsequently it is adaptable. They created a novel algorithm by utilizing the idea of dynamic boundary area to backing consistent ISHO between the 3G and WLAN. Their results show that the proposed limit territory based ISHO algorithm beats the current WLAN ISHO and 3G algorithm.

Bittau et al.[10] present a novel defenselessness technique which permits an attacker to send subjective information on a WEP in the wake of having listened stealthily on a solitary information packet. They present WEP re-keying avert conventional attacks. Xing et al. [11] propose an enhanced form of 802.11i to make more DoS safe. Because of the physical weakness of WLAN links, Dos attacks dependably survive from end to end frequency sticking, system sticking, or different endeavors. Nashon et al.[12] propose an incorporated ISM security model that consolidates a go down arrangement to shield against Dos attacks. Furthermore the creator accepts the use of CCMP to give Confidentiality and Integrity and utilization EAP TILS or 802.11 xs by means of RADIUS to give confirmation. They utilized simulation as a part of OPNET to demonstrate that their security model performs better to give enhanced security as far as privacy, respectability, validness and accessibility. Omar et al. [13] propose a straightforward, effective security overlay protocol to existing 802.11 systems. Beck et al. [14] described innovative attacks next to TKIP base IEEE 802.11 systems . They characterized new outlines to ceaselessly produce new key streams, which permit more and more packets to be infused. They introduced an attack next to the Michael message respectability code. The authors in [15] give a suggestions guide for remote LAN security. Security of the remote system is a vital issue, on the grounds that the transmission media is open. They created aide for the security purposes, security protocols begins by choosing the system size relying upon the number of the computers on the system with different size(little, medium and substantial) has diverse arrangements for security. Mavridis et al.[16] concentrate on three principle security conventions WEP, and WPA2, WPA . They talked about and displayed in detail an analytical method towards WEP and WPA2 cracking from

genuine circumstances. They show that any remote system may be experiencing effective hacking endeavors, in the event that it is not deliberately setup and secured. Tsukaune et al. [17] proposed a protected WEP operation next to key recuperation attacks. They proposed a strategy that require for attackers no less than 100,000 packets to recuperate the WEP key. Poddar et al. [18] present an investigation of WEP, and WPA2, WPA. They have attempted in the direction of carry out and make sure validation of each of the protocols by inferring the legendary attack vector script by Air break set of apparatuses. The examination is directed on Back Track working framework which is considered as devoted pretesting working framework. In the test outcome, they discovered that WEP is the weakest, to which WPA was a makeshift arrangement and WPA2 is an exceptionally strong and long team arrangement. Ifeyinwa et al. [19] comprehensively assessed different improved protocols to WEP connected confirmation, secrecy and respectability issues. The author discovered that quality of every arrangement relies upon how fit the encryption, confirmation and respectability strategies work. They utilize a Defense in Depth Strategy and joining of biometric in 802.11i. Adib and Raissouni [20] have introduced security architecture toward implementing AES algorithm. The study was carried out in FPGA and finds more suitability in implementing in WLAN. Sodho et al. [21] have proposed a unique key management for securing wireless network where the focus was more on storage of keys. However, the applicability of the work in WLAN is not discussed much.

1.2 Problem Identification

The identified problems of the proposed study are as follows:

- **Security protocols**: The resiliencies of the existing security protocols are highly questionable in area of WLAN. Still there is a prevalence of using WPA and WEP as the core security technique in access point. It is already known that both of them are vulnerable for various lethal attacks particularly wormhole attack and Sybil attack, where identities and routes are easy to be compromised.
- **Role of Access Point**: Majority of the existing protocols discussed in prior section discusses about security techniques on the client's machine. The role of access point is not that much emphasized. It is noticed that access point is considered as mere a router to help in communication of the nodes present in WLAN. It should be known that access point in WLAN is the most vulnerable point as all the data transact through it and it is also responsible for authenticating and authorizing other nodes. Hence, existing studies focuses only on physical level security and not on application or network layer security. Hence, there is an emergent need of multilayered security technique to secure data in WLAN.
- **Selection of Encryption Standard**: It was seen that SHA is the most frequently used cryptographic technique in WLAN, which is followed by AES. There is no doubt that SHA as well as AES has potential merit factor as an encryption standards in WLAN, but there are certain pitfalls too. SHA is computationally slow and yield larger hash size, where AES design is quite complex. However, AES supports faster processing in hardware and hence a slight modification in AES could solve the issues of encryption.
- **Compliance to Security Standard**: Although it is quite a challenging task to ensure privacy, confidentiality, and integrity in security protocols in WLAN, but it is indeed demanded for ensuring optimal security. If any cryptographic algorithm ensures so then its design can be expected to be highly complex. Hence, there is a need of a lightweight cryptographic technique as well as logical technique that can ensure maximum compliance of security standards and less computationally complex in WLAN. Or else attacks cannot be mitigated to maximum extent.

Hence, the present research work introduces a multilayered security technique to secure data communication in WLAN.

1.3 Proposed Model

The prime aim of the present study is to incorporate maximum level of security to the data that are being transacted through various WLAN routers. The proposed model is an extension of our prior model SAKGP (Secured Authentication of Key Generation Protocol) in WLAN [22]. SAKGP have introduced a unique technique for ensuring the authentication of bidirectional nature with an aid of mathematical model. SAKGP also adopts the latest version of cryptographic hash function (SHA-3), that was never tried before. The present system is coined as MDS-WLAN which stands for Maximal Data Security in WLAN to introduce a most robust, simple, as well as cost effective security techniques to ensure privacy, integrity, and confidentiality against wormhole attack and Sybil attack. The schematic architecture of the present system is highlighted in Figure 1. The present system targets to accomplish the maximal standards of security with privacy, confidentiality, and non-repudiation using lightweight AES encryption standards.

2. RESEARCH METHODOL

The proposed system has considered empirical as well as mathematical modelling as the standard of research methodology. The presented MDS is designed considering the real-time scenario where WLAN is used like institution, campus, cafeteria etc. using multiple access point as well as multiple terminals with some of the latest configurations. The primary components of present system are i) Sender node, ii) Receiver node, and iii) access points. The layout of the evaluation of MDS is shown in Fig.2. The primary role of access point is to manage the node identities. Usually, in real-time the node creates its ID in WLAN configuration, but in present system, the access point will create a significant node ID that are maintained privately by them and common terminals doesn't have any sort of access to such private information. This formulation plays a significant role in data security as well as key management uniquely. For an example, consider an environment where there are 16 keys being randomly distributed among 16 users, where none of the 16 users knows any information about their neighbor keys. This principle plays a significant role in mitigating wormhole and Sybil attack as the identities of the nodes cannot be compromised. The attacker will have to guess with some complex algorithms to find the location of keys. The common cryptographic technique stores keys in storage, but the present MDS stores keys in network.

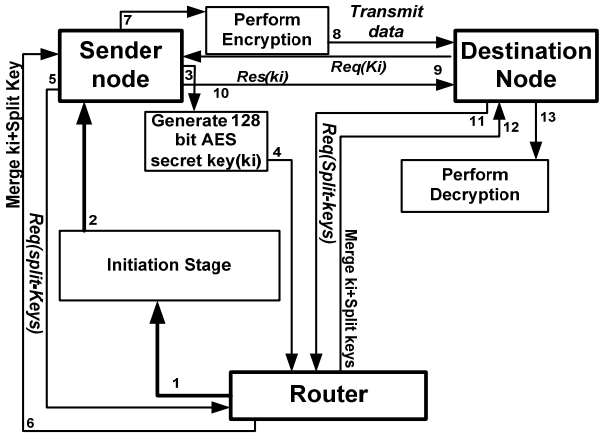

Figure 1 Schematic Architecture of MDS

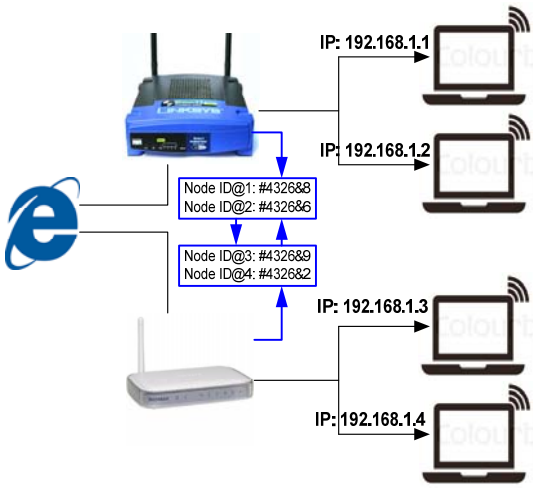

Figure 2 Layout of the MDS

Every time the sender node would like to communicate with destination node, access point plays a critical role. Without the access point, no one will able to retrieve the keys from the network. For giving an access to the sender, the access point need to merge the secret key of sender and response of split keys. Even by default, if the access point is also compromised, the intruder will never be able to guess the location of secret keys or can generate split keys. Hence, the proposed system is also resilient against problem of rogue access point. For incorporating effective design principles, we have designed it in Java environment with enrich APIs of networking and cryptography to carry out the present study. The present study also offers higher level of communication performance due to adoption of AES based encryption

2.1 Implementation Scenario

The implementation of the proposed MDS-WLAN system is done on real-time test bed. The tabulated information in Table 1 also pertains to the security protocols supported by access points as well as IEEE standards supported by the terminals. The experimentation of the present system was done considering all G-based wireless routers. Table 1 highlights the specific configurations of the access points as well as terminals used for testing the present protocol.

The present study considers 12 different domains that are individually handled by the access points for 59 users are considered. Two significant algorithms are created in this study. Algorithm-1 is responsible for node activation, while Algorithm-2 is responsible for data security. The design of the Algorithm-1 is done considering the fact that either one or more than one node are sending request to the WLAN router. After the access point's gives access priviledge to the requester node, simultaneously, the access point will also require checking the number of node activation in network. The meaning of the term node activation means the nodes are provided with authenticated secret key to perform communication with each other.

Table 1 Components used for Experiments

Components	Type	Security Protocol	Numbers
WLAN Routers	Linksys-WRT54G-802.11g	WEP, WPA, WPA2	7
	Netgear-WGR614	WPA, 128-bit WEP	5
Components	Type	IEEE	Numbers
Terminals	Lenovo Notebook	802.11a/b	14
	Lenovo ThinkPad	802.11 b/g/n	15
	Dell Latitude (D610)	802.11b	19
	Dell Latitude (D400)	802.11b	11

Hence, using our prior SAKGP technique, if there is only one node, there is no reason to perform authentication as SAKGP already ensured robust authentication from one access point to one terminal using bidirectional keys sharing. However, if there are presence of more than 2 nodes, the access point will generate 128 bit of AES secret key sharing (line-8 of Algorithm-1) and perform splitting of the secret key to be distributed within the network (Line-11 of Algorithm-1). One of the interesting point in present model is that access point will manage the explicit records of the secret key by giving unique node ID to each node (Line-12), which is of private type. Hence no other nodes in the network can ever access that information rendering potential node ID to ensure the privacy of access point which indirectly maintains higher level of confidentially in multihop communication process in WLAN with higher number of nodes. Another unique point to be noted in the design principle of Algorithm-1 is that the secret key can be splitted in only 2 or 16 parts as the minimum size of one block of message occupies around 8 bit to support 128 bit of encryption using AES (so, 8x16=128) (Line-13). We choose to work on AES as this is frequently adopted cryptographic hash function in normal wi-fi environment like office, campus, cafeteria etc. After receiving the secret key, the requester node is allowed an access to the network. It is critically important for us to incorporate algorithm-1 to avoid rogue access point as well as for proper identification of legitimate nodes in WLAN environment

2.2 Algorithm for Node Activation

The present system ensures optimal security by adopting a simple and yet cryptographic mechanism considering only three entities, source node (i_s), destination node (i_d) and access point (router). After the requester node(i_s) obtain activation state from the Algorithm-1, it can communicate with the destination node (i_d) using Algorithm-2. According to Algorithm-2, any node in the network can initialize a message as a source node to the access point, where the source node will be required to select the IP address of the destination node and this information has to be forwarded to the access point. The prime reason behind this is that access point is a node considered in the network that has secured information about the source and destination nodes. The source node will generate their own 128-bit AES secret key (Line-3 of Algorithm-2) and will send a request message to the access point about the splitted key (Line-4 of Algorithm-2). The source node will be authenticated by the access point, which upon successful authentication, the access point will retrieve the splitted key from the network (Line-5 of Algorithm-2). Hence, it can be seen that secret keys resides in network and access point can only generate it whenever the request is made by sender node (i_s).

Algorithm-1 for Node Activation
Input: request message for authentication (i_{req}), requester node (i), Access point (router)
Output: Authorization for requester node.
Start
1. Node *i* request i_{req} to join the network
2. i_{req}→router.
3. Perform authentication
4. **If** i=1,
5. No authentication
6. **Return**;
7. **If** i⩾2,
8. router→hash(s_k) //AES secret key
9. u=hash(s_k); //s_k=Secret key
10. **Break**;
11. Distribute *u* to $i_{n.}$ //n=total number of nodes
12. Generate Priv(ID)→i_n.
13. Split *u* to Rand(i_n) (2<i<16)
14. Activate the node *i*
End

2.3 Algorithm for Maximal Data Security

After the access point retrieves the responses, it merges the key (k_i) from the sender node (i_s) and response Res($msg_{splitkey}$) that it has retrieved recently (Line-6 of Algorithm-2). The concatenated result (v_s) of this operation is send to the sender node. The sender node will perform encryption of the message twice, where the first level of encryption will be carried out using secret key (k_i) of the sender node itself (Line-9 of Algorithm-2) and second level of encryption will be carried out using splitted key (v_s) that is recently received from access point (Line-10 of Algorithm-2). Obtaining the proper update about the destination node by the access point, sender node can now transmit data to the destination node. The destination node, after receiving the encrypted data, will request sender node for their own secret key (k_i). Then the destination node requests the access point for splitted key (v_s) of the source node as it will be always in possession of access point. Upon receiving the request, the access point will perform authentication of the destination node and retrieve source node splitted key from the network. Finally, the access point merges the splitted key (vs) and response and the concatenated outcome (v_d) will be forwarded as a new splitted key to the destination node (Line-17 of Algorithm-2). Upon receiving the splitted key, the destination node also performs dual step decryption process. The first level of decryption process is mechanized by splitted key of source node (Line-19 of Algorithm-2) and the second level of the decryption process is mechanized by secret key of source node (Line-20 of Algorithm-2).

Algorithm-2 for Maximal Data Security (MDS)
Input: IP address of i_d,
Output: Successful and Secure data transmission
Start
1. Initialize source node is and destination node i_d.
2. $i_s \rightarrow$StringCapture(IP of i_d) to router
3. i_s generates k_i (size of i=128)
4. $i_s \rightarrow$Req($msg_{splitkey}$) to router
5. router validate Req($msg_{splitkey}$) and retrieves Res($msg_{splitkey}$)
6. router$\rightarrow v_s$ = cat(k_i|| Res($msg_{splitkey}$))
7. Send v_s to i_s
8. Initiate dual encryption by i_s
9. i_s: (E_{S1}=encrypt(k_i))
10. i_s: (E_{s2}=encrypt(v_s))
11. i_s transmit data to i_d.
12. i_d received encrypted data from i_s.
13. $i_d \rightarrow$Req(k_i) to i_s
14. $i_s \rightarrow$Res(k_i) to i_d
15. $i_d \rightarrow$Req(v_s) to router
16. router authenticated i_d and retrieve v_s from network
17. router$\rightarrow v_d$= cat(v_s|| Res($msg_{splitkey}$)) to i_d
18. Initiate dual encryption by i_d
19. i_d: (E_{S4}=encrypt(v_d))
20. i_d: (E_{S3}=encrypt(k_i))
End

The prime objective of the proposed algorithms discussed in present study is to incorporate multilayer security protocol for WLAN under most challenging environment. The present system is compared with the most frequently adopted cryptographic protocols in WLAN i.e. SHA and AES. The present study offers a simple and yet a robust protocol for performing encryption as well as decryption as explained in the previous section. It is known that a typical cryptographic algorithm has various iterative steps and hence it can ensure highest level of security. However, ensuring the communication and service relay is another performance factor that should be evaluated while framing cryptographic protocol. The next section discusses about the result accomplished from the study.

3. RESULT DISCUSSION

The result accomplished from the proposed study is discussed in this section with respect to throughput, latency, and packet delivery ratio. Throughput is evaluated by considering the amount of the data packet being transmitted from the sender to the receiver. Hence, we calculate the throughput by estimating the rate of generation of the keys for validating the user that enables them to forward the data packets with respect to the request being made by the 59 users involved in the experiment. Table 2 highlights that AES has better throughput performance recorded in observational time in seconds compared to SHA. AES

algorithm is highly resistive against any brute force attack, but owing to extensive inclusion of complex mathematical designs, AES could be slower too. SHA algorithm on the other hand is found to be better alternate for security for AES as it produces long hash value, something which AES cannot produce. Although SHA supports higher security protocols, but it doesn't support enhancement of performance in large scale WLAN system in real-time. Table 2 shows that overall throughput performance of AES is found to be always better compared to SHA versions. The proposed system revises the structure of AES to generate the split keys in such a way that it has bi-directional nature; it is light weight (128 bit), and supports optimal security on real-time terminals included in our experiment. Hence, better non-repudiation policy can be ensured by the present system along with data packet integrity.

Table 2 Throughput Analysis

Time(Sec)	SHA	AES	AES with MDS
0.07412	1.74	2.24	3.86
0.11657	1.80	2.39	3.91
0.16013	1.84	2.34	3.96
0.1017	2.01	2.49	3.98
0.18681	5.74	2.24	7.98
0.23037	5.80	6.39	8.06
0.27203	5.84	6.34	8.17
0.3145	6.01	6.49	9.24
0.40061	9.74	7.24	9.96

Table 3 highlights the latency analysis of the present system. The present model MDS with AES has reduced latency factor compared to conventional AES and SHA algorithm in cryptography. Hence, the outcome highly encourages the system to be used in more large scales without any fear of compromization by intruder.

Table 3 Latency Analysis

Time(Sec)	SHA	AES	AES with MDS
0.481667	4.49	3.49	2.01
0.585278	9.19	6.49	6.03
0.620815	13.19	10.49	10.01
0.632000	17.74	16.34	13.74
0.633665	17.89	16.39	13.89
0.634306	17.84	16.44	13.84
0.637084	18.01	16.49	14.28
0.647447	22.79	21.29	14.79
0.65454	25.49	24.01	18.79

Table 4 Data Packet Delivery Ratio Analysis

Time(Sec)	SHA	AES	AES with MDS
1	3.96	4.86	5.46
5	4.01	5.01	5.61
20	8.23	9.31	14.31
30	10.37	14.04	19.00
40	14.11	18.31	19.84
50	20.19	21.41	22.62
60	24.05	25.03	26.31

To check integrity of the data packet, packet delivery ratio is computed by amount of the test file already received by the destination node to the amount of total files already sent by the sender node. Finally, we evaluate the time required to transmit the data packet by dividing number of bits by rate of data transmission. For better precision analysis, we have used WireShark [23] that monitors the real-time data transaction on the experimental test-bed of MDS. Table 4 shows the outcome of the packet delivery ratio, where it can be seen that performance of AES with proposed MDS is much better compared to conventional SHA and AES. The results obtained show the justification of using modified AES to support security in WLAN.The conventional research outcomes on network security is tested for processing time that gives the scale of computational time complexity. We have shown extensive analysis by observing the computational time complexity of each phases of algorithm implementation. The computational time complexity of the present MDS algorithm is studied with respect to i) activation time, ii) validation time, and iii) time required to perform encryption. Hence, it can be seen that proposed technique excels better as compared to the existing security standards using SHA as well as frequently used AES algorithm in the wireless routers. The outcomes in the tables above exhibits that it not only ensure better security but also optimizes the networking and communication performance of the WLAN. The algorithm is very light-weighted for which reason the storage complexity is quite less. Hence, it can support the terminals even in presence of lethal threats on WLAN.

Figure 3 highlights the analysis of the activation time. Basically activation time pertains to time required to execute the Algorithm-1. We compare our results with SHA-1/2, as it is the most frequently used algorithm in many existing studies e.g. [24], [25] etc. The outcome shows that with increasing number of

access point (we have implemented on 16 access points) considered in the study, SHA1/2 consumes much extra time to generate the split keys compared to the present MDS. The prime reason is SHA1/2 uses 160 bit of message generation hence the size of the message becomes quite heavy for splitting operation of the key. The similar operation in present MDS using AES uses only 128 bit size, hence, activation of the node becomes quite faster. Once the node is activated by the router, then it can communicate with other nodes in WLAN system. The curve of MDS is found to be quite stable and almost linear whereas, the curve of SHA1/2 increases more as increased number of dependency of communication on access point.

Figure 4 highlights the outcome of the validation time which pertains to operation time of Algorithm-2. The operation time of Algorithm-2 has two types of steps, one for sender node and other for destination node. In the entire operation of Algorithm-2, the router has to retrieve the secret keys as a response against the request from both sender node as well as destination node. This typical case of key management doesn't require to store the key in any physical device as the key has to be retrieved from the network itself. Therefore, a much reduced storage or memory is required in the entire process of proposed MDS technique. Hence, the validation time significantly reduced compared to SHA1/2 protocol. The outcome showcase the evidence of non-repudiation of the proposed system, which is significantly better compared to SHA1/2.

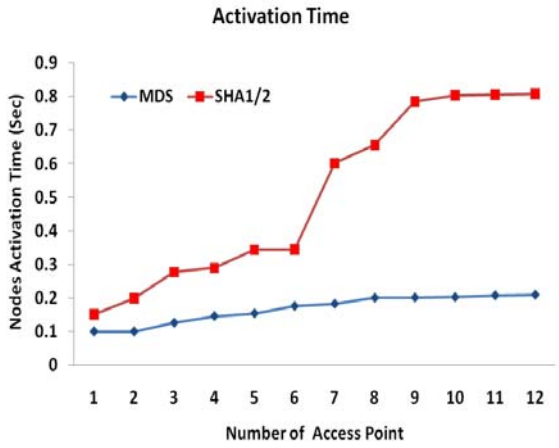

Figure 3. Analysis of Activation Time

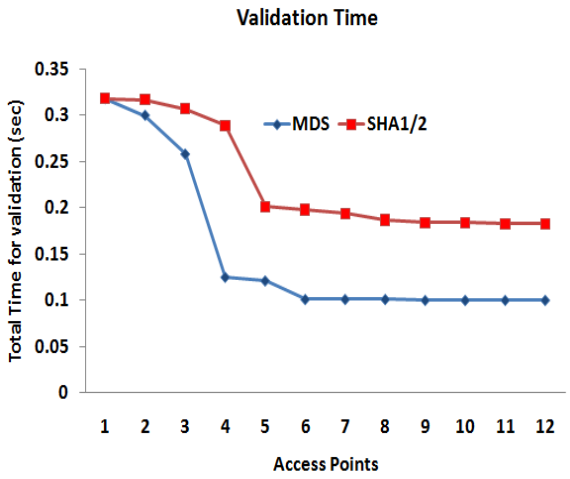

Figure 4. Analysis of Validation Time

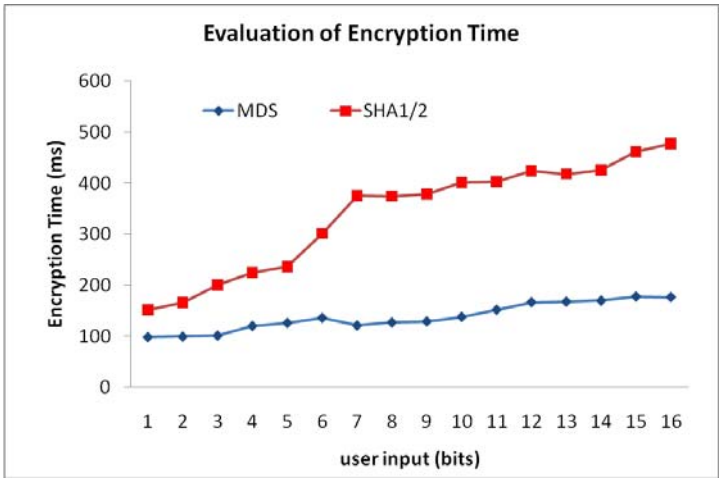

Figure 5. Analysis of Encryption Time

Figure 5 shows the time required to perform only encryption of the data packet particularly in Algorithm-2. Algorithm-2 design principle shows that the access point concatenates the key of the sender as well as response message. The similar operation is also carried out in decryption stage, but with reduced

dependency of secret key from sender node owing to Algorithm-1. Hence, the encryption time doesn't take much time for encrypting data with increasing numbers of the user inputs of 16 bits. Hence, on every encryption, the operational steps speeds up by using AES algorithm that runs quite faster compared to SHA1/2 on hardware. Although SHA version supports 160 bits of message, but AES is also scalable to more than 168 bits of message. The 128 bit block size of AES in the proposed system renders the faster encryption mechanism as compared to frequently used SHA versions in cryptographic hash function. Hence, the proposed algorithm not only supports potential security standards but also supports higher communication performance.

4. CONCLUSION

The primary outcome of the proposed system shows that the presented algorithm provides highly efficient techniques not only towards maximized data security but also enhances the communication performance in WLAN in most cost effective manner. Ensuring security over WLAN is one of the most critical challenges encountered by the users worldwide. Although most advance sections of wireless networking system are a thorough part of investigation in research community, but still the most practically adopted WLAN is encountering security threats. The present study has introduced a security protocol which is not only light weighted but also potentially secure against various types of lethal threats on WLAN. This paper has presented mainly two algorithms that is the backbone of the study. The first algorithm ensures that every node in the environment are legitimate and are authorized communication. A unique feature of this paper is the access point maintains the unique node ID privately that cannot be accessed by any other node present in the network. The proposed technique also offers the best security features even if the secret key is compromised then also data cannot be decrypted by the intruder as it has higher level of dependency of the splitted keys, which are never shared with other nodes present in the network. The outcome of the proposed technique is compared with existing security techniques like AES, SHA1/2 that are frequently used in WLAN. The results show that proposed MDS scheme provides optimal security with superior communication performance.

REFERENCES

[1] Y. Zhang, H. Zheng, M. Ma IGI.Handbook of Research on Wireless Security. V.1 *Technology & Engineering*. 2008; 860
[2] R. Prasad, S. Dixit, V. Nee, A. Ojanpera. Artificial intelligence Globalization of Mobile and Wireless Communications. *Springer*, 2010; 356
[3] M. Finneran, F.D. Jonathan, T. Finneran. Computers the Privacy Engineer's Manifesto. *Springer*. 2014; 104
[4] Baek, Hyun K, Smith. S.W and Kotz. D. A Survey of WPA and 802.11 i RSN Authentication Protocols. *Dartmouth Computer Science Technical Report*. 2004
[5] S. Mukesh, R. Bai, Y. Lin, Y. Wang, W. Yang, and Q. Zhang. Key management protocols for Wireless Networks. Lab for Advanced Networking. Dept of Computer Science. University of Kentucky, *Technical Report.* 2004
[6] A. Kumar, and A. Aggarwal, Charu. Survey and Taxonomy of Key Management Protocols for Wired and Wireless Networks. *International Journal of Network Security & Its Applications*. 2012; 4
[7] G. Kambourakis, A. Rouskas, S. Gritzalis, and D. Geneiatakis. Support of subscribers' certificates in a hybrid WLAN-3G environment. *Computer Networks*. 2006; 11: pp.1843-1859
[8] A. Balachandran, G.M. Voelker, and P. Bahl. Wireless hotspots: current challenges and future directions. *Mobile Networks and Applications.* 2005; 3: 265-274
[9] S. Mohanty. A new architecture for 3G and WLAN integration and inter-system handover management. *Wireless Networks.*2006; 12: 6, 733-745
[10] A. Bittau, M. Handley, and J. Lackey. The final nail in WEP's coffin. *IEEE Symposium In Security and Privacy*. 2006; 15
[11] X. Xing, E. Shakshuki, D. benoit, T. Sheltami. Security Analysis and Improvements for IEEE 802.11 i.*In The 12th Annual Network and Distributed System Security Symposium (NDSS'05) Stanford University.* Stanford. 2005; 90-110
[12] O.N. Ondiwa, E. Biermann, and G. Noel. An integrated security model for WLAN. *In AFRICON*. 2009; 1-6
[13] Y. Omar, M. Youssef, and El Gamal..H. ARQ secrecy: From theory to practice." *In Information Theory Workshop, IEEE*. 2009; 6-10.
[14] M.Beck. Enhanced TKIP michael attacks. *arXiv preprint* arXiv:1410.6295. 2010
[15] J. Padgette, K.Scarfone, and L. Chen. Guide to Bluetooth security. *NIST Special Publication*. 2008; 121
[16] I.P. Mavridis, H. Androulakis, B. Halkias, and P. Mylonas. Real-life paradigms of wireless network security attacks. *In Informatics 15th Panhellenic Conference*. 2011; 112-116
[17] T. Tsukane, Y. Todo, and M. Morii. Proposal of a Secure WEP Operation against Existing Key Recovery Attacks and its Evaluation. IEEE-Information Security (Asia JCIS), 2012 Seventh Asia Joint Conference.2012; 25-30
[18] V. Poddar and H. Choudhary. A Comparative Analysis Of Wireless Security Protocols (Wep And Wpa2). 2014

[19] Ajah .A Ifeyinwa. Evaluation of Enhanced Security Solutions in 802.11-Based Networks. *International Journal of Network Security & Its Applications*. 2014; 4
[20] S.A Adib, N. Raissouni. AES Encryption Algorithm Hardware Implementation Architecture: Resource and Execution Time Optimization. *IAES-INternational Journal of Information and network Security (IINS)*. 2012; 1:2
[21] A.H. Sodhro, Y. Li, M.A. Shah. Novel Key Storage and Management Solution for the Security of Wireless Sensor Networks. *IAES-TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2013; 11:6
[22] P.H. Latha, R. Vasantha. SAKGP: Secure Authentication Key Generation Protocol in WLAN, *International Journal of Computer Applications*. 2014; 96: 7
[23] https://www.wireshark.org/
[24] J. Eisinger, P. Winterer, B. Becker, *Securing Wireless Networks in a University Environment*. IEEE International Conference on pervasive Computing and Communication Workshop. 2005; 312-316
[25] G. Epiphaniou. Iterative Block Cipher's effects on Quality of Experience for VoIP Unicast Transmissions under Different Coding Schemes. *Doctorial Dissertation of University of Bedfordshire*. 2010

BIOGRAPHIES OF AUTHORS

Mrs. Latha P.H. is currently working as an Assistant Professor in Atria Institute of Technology, Bangalore (India) in Department of Information Science. She has total of 15 years of teaching experience. She has completed her Masters of Technology in Computer Network Engineering at AMC College of Engineering and at present is pursuing her research programs from Visvesvaraya Technological Institute, Belgaum. She has won various recognition in the are of networking as well as software testing. She has a special interest on security issues in wireless networking.

Dr. Vasantha has completed her PhD on 1985 from Indian Institute of Science. She has completed hase Masters of Science in 1978 from Manasa Gangothri Mysore University. She has 35 years of work experience in teaching and has made some significant contributions in the area of academics. She has also worked as Assistant Professor in University of Okhlahoma, USA, as well as in University of Cleveland, USA. At present, she is working as Professor in Sambhram Institute of Technology