www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 03, March 2023, pp : 123-130

e-ISSN : 2583-1062

Impact Factor : 5.725

DESIGN OF SECURE WIRELESS LAN USING MODIFIED TEMPORAL KEY INTEGRITY PROTOCOL

Shubhi Danpati[1], Mr. Shailesh Khaparkar[2]

[1]M.Tech. student, GGITS, Jabalpur, India.

[2]Associate Professor, GGITS, Jabalpur, India.

ABSTRACT

Wireless Local Area Networks, or WLANs, are an attractive and cost-effective way to get started with mobile computing. They enable computers to move around without using cables and communicate at speeds comparable to those of wired LANs. In terms of the network's security, these features came at a high cost. These security issues and their solutions are identified and outlined in this work. The first logical approach to securing WLANs was Wired Equivalent Privacy, or WEP. The new encryption base security protocols known as Kerberos and TKIP (Temporal Key Integrity Protocol) are currently in use in WLANs and can be considered an advancement of WEP. However, the time required for encryption and security in this advance WEP is still sufficiently high, thereby reducing the total amount of time required for WLAN communication. Solutions that combine Kerberos and minimize TKIP into MoTKIP are proposed for faster and more secure WLAN communication. The design of the proposed work is done in MATLAB, and the results are calculated using Avalanche and time delay.

Keywords: WEP: Wired Equivalent Privacy, TKIP: Temporal Key Integrity Protocol, SHA: Secure hash algorithm, KEAP: Kerberos extensible authentication protocol, DoS: Denial of Service.

1. INTRODUCTION

Access to wireless networks at data rates that were acceptable was made possible by wireless local area networks (WLANs). IEEE802.11 is the driving technology standard for WLANs, and the Institute of Electrical and Electronics Engineering (IEEE) has established standards and specifications for data communications in a wireless environment [1]. Since WLANs are used as an extension of the existing fixed/wired LANs, it is important to raise their security to levels comparable to or higher than those of wired LANs because of their distinct nature. In general, IEEE802.11 can function in either the Ad hoc or Infrastructure network topology modes. The infrastructure mode of WLANs is the subject of this paper. A wireless local area network (WLAN) is created when wireless stations (STAs) communicate wirelessly with a network access point (AP) that is connected to the wired network. There are three stages involved in the creation of connections between AP and STAs: association, authentication, and probing [1].

2. METHODOLOGY

According to the findings of the study, the proposed work will design a network that makes use of a singular combination of Kerberos and Temporal Key Integrity Protocol (TKIP). The initialization vector (IV) used in the encapsulation process is effectively increased to 48 bits by TKIP. By increasing the number of possible IV values from 224 to 248, the likelihood of an IV being reused is significantly decreased. Additionally, WEP's weak key vulnerability is addressed by increasing the IV length. This is accomplished by employing a novel technique for dividing the IV into two parts. To create a 24-bit IV without using weak keys, the first 16 bits of the IV's least important part are padded. The term for this procedure is "per-packet key mixing." The TKIP IV's remaining 32 most significant bits and the wireless LAN card's MAC address are used to calculate a mixed key that is joined to this IV. It guarantees that each packet contains a distinct set of IVs. As a result, the WEP algorithm's primary issue—that each station in the network uses the same key to encrypt data—is resolved.

3. PROPOSED TKIP

The second phase of the TKIP key mixing function reuses the 80-bit TKIP-mixed Transmit Address and Key (TTAK) or phase 1 key (P1K) with MAC Protocol Data Units (MPDUs) associated with the same 32-bit upper IV-part Temporal Key (TK) and Transmitter Address (TA) for the following 216 packets. This process is depicted in Figure 1. As a result, the receiver knows about the 32-bit high IV when the first encrypted packet is sent. This part is cached because it stays the same for the next 216 packets. The final WEP seed, also known as the per-packet key, is created when the output of the first phase is mixed with that of the TK and a 16-bit low IV-part counter is continuously incremented (from 0x0000-0xFFFF). It is unnecessary to send the full 48-bit extended IV as redundancy once more in each packet because the receiver already knows about the 32-bit high IV and the 16-bit low IV sequence. As a result, the cached 80-bit TTAK derived from the IV in the first packet at the transmitter will also serve as the same input to the receiver's second phase mixing, and the subsequent 16-bit IV counter will simply increment by one unit. Phase 2

www.ijprems.com
editor@ijprems.com

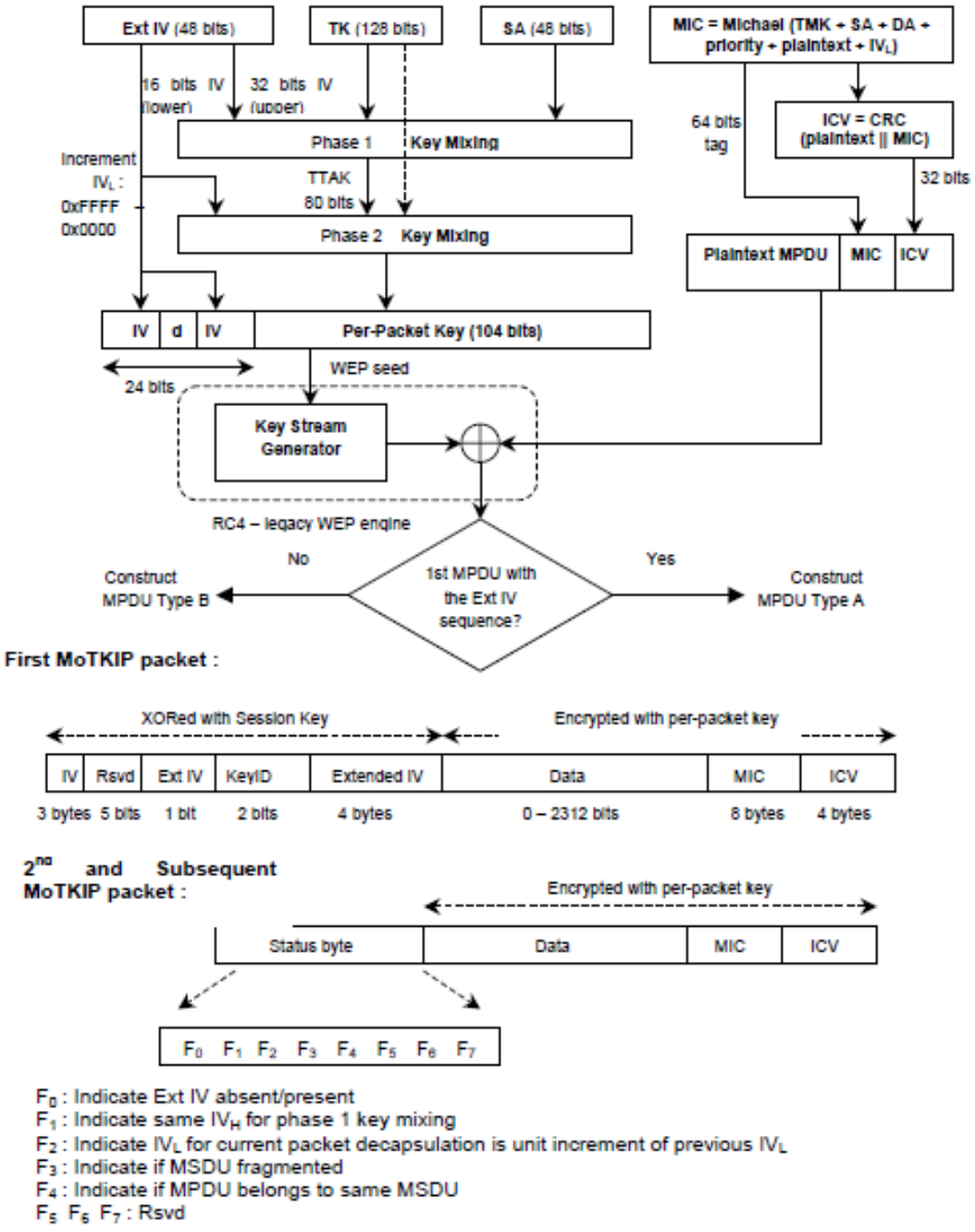
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 03, March 2023, pp : 123-130

e-ISSN : 2583-1062

Impact Factor : 5.725

can be computed in advance while waiting for the subsequent packets to arrive at the receiver because the IV counter is predictable. As a result, the redundant extended IV of four bytes is removed from the packet load in the new Modified TKIP (MoTKIP) frame format for packets from the second to the 216th. To optimize the TKIP key mixing phase, we employ the standard code algorithm from the 2004 IEEE Standard for Information Technology.



F_0 : Indicate Ext IV absent/present
F_1 : Indicate same IV_H for phase 1 key mixing
F_2 : Indicate IV_L for current packet decapsulation is unit increment of previous IV_L
F_3 : Indicate if MSDU fragmented
F_4 : Indicate if MPDU belongs to same MSDU
F_5 F_6 F_7 : Rsvd

Figure 1 Modified TKIP (MoTKIP)

This is a significant improvement over the previous WEP protocol, which relies on the insecure RC4 stream cipher. Counter Mode AES encryption (CTR-AES) and Cipher Block Chaining – Massage Authentication Code (CBC-MAC), both based on AES, make up CCMP. By calculating the message's Message Integrity Code (MIC), CBCMAC ensures data integrity and authenticates the sender, while CTR-AES encrypts the transferred data (thereby ensuring confidentiality). Figure 2 depicts how MIC is calculated using the AES block cipher-based CBC-MAC algorithm.

The process of feeding the cipher text output from the first round of CBC-MAC back into the second round of CBC-MAC as an input continues until the nth round. The plain text's MIC is the nth round's output. KCK, derived from PTK and used to calculate MIC, is shared by STA and AP and is 128 bits minimum. Assume that the MIC that is produced by AP is referred to as the MIC that is produced by STA. In addition to the initial message, MIC(STA) will be transmitted to the AP. The initial message will be received by the AP, which will then compare the calculated MIC(AP) with the calculated MIC(STA).

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 03, March 2023, pp : 123-130

e-ISSN : 2583-1062

Impact Factor : 5.725

CTR-AES encryption uses the counter value, TK, the message, and MIC. In addition, CCMP-specific headers are created. Information like PN in the CCMP header is necessary to defend against replay attacks. When the CCMP protocol is used, Extended IV is a one-bit flag that is always set to one. The message and its MIC in encrypted form are the final outputs of the CCM encryption block. Next, a MAC header is added—some parts of the MAC are already present in the MIC to ensure authenticity and integrity—and a CCMP header is injected between the encrypted message and the MAC header. The insecure channel is now being used to send the encrypted message packet with its MIC, CCMP, and MAC headers. The message and MIC will be decrypted by the receiver using TK, and a new MIC will be created from the decrypted message and some parts of the MAC header. The two MICs are compared to ensure the message's validity and the sender's authenticity. CCMP makes effective use of PN; Problems with WEP and its successor, TKIP, can be solved with the assistance of PN. For each message, a new PN must be created by continuously increasing it. When TK is changed, PN must be initialized to one, according to IEEE802.11i. The PN number is compared to the previous PN number that was received by the receiver; if the new one is greater than the previous one while employing the same TK, this indicates that the message is not under replay attack. Increasing PN for each message will ensure that the same TK will never be used again.

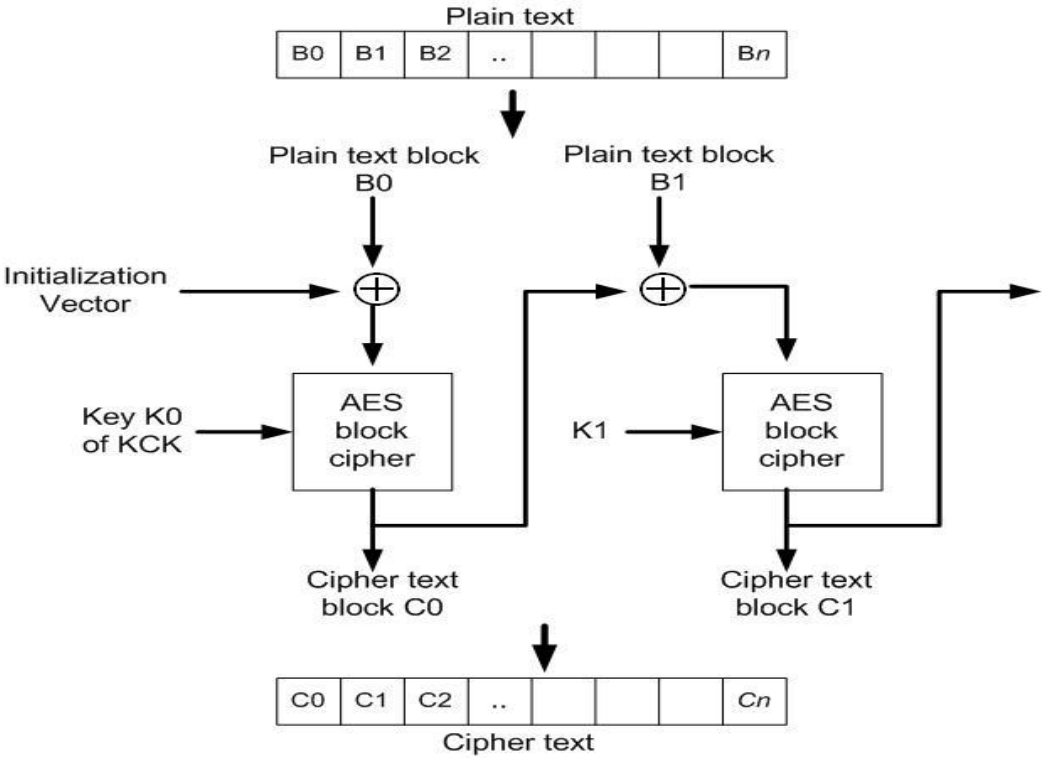


Figure 2 Illustration of Calculation of MIC using CBC-MAC AES based bloc cipher CTR-AES

Proposed block description: The following steps can be used to explain the work flow: Step 1: First, create 256 nodes that can generate IEEECBC-MAC Protocol packets with each node's unique MAC address.

Step 2: Now, create a star network with all 256 nodes and begin sending and receiving data from each node. Check to see that the data is properly received at each other node; this is a WLAN network.

Step 3: For creating security issues in the proposed WLAN, add logical and physical attacks. Physical attacks include rogue access points, AP coverage, and the physical location of APs; logical attacks include: Step 4: Spoofing of MAC addresses, WEP attacks, and a denial-of-service attack Step 5: Send packets using the modified temporal key integrity protocol (MoTKIP), the proposed security protocol. If you're on a public network, send data packets encrypted by Proposed AES-enabled Kerberos.

Step 6: compute the time delay and avalanche between the data in the original packet and the secure output that is produced using the proposed AES Kerberos

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 03, March 2023, pp : 123-130

e-ISSN : 2583-1062

Impact Factor : 5.725

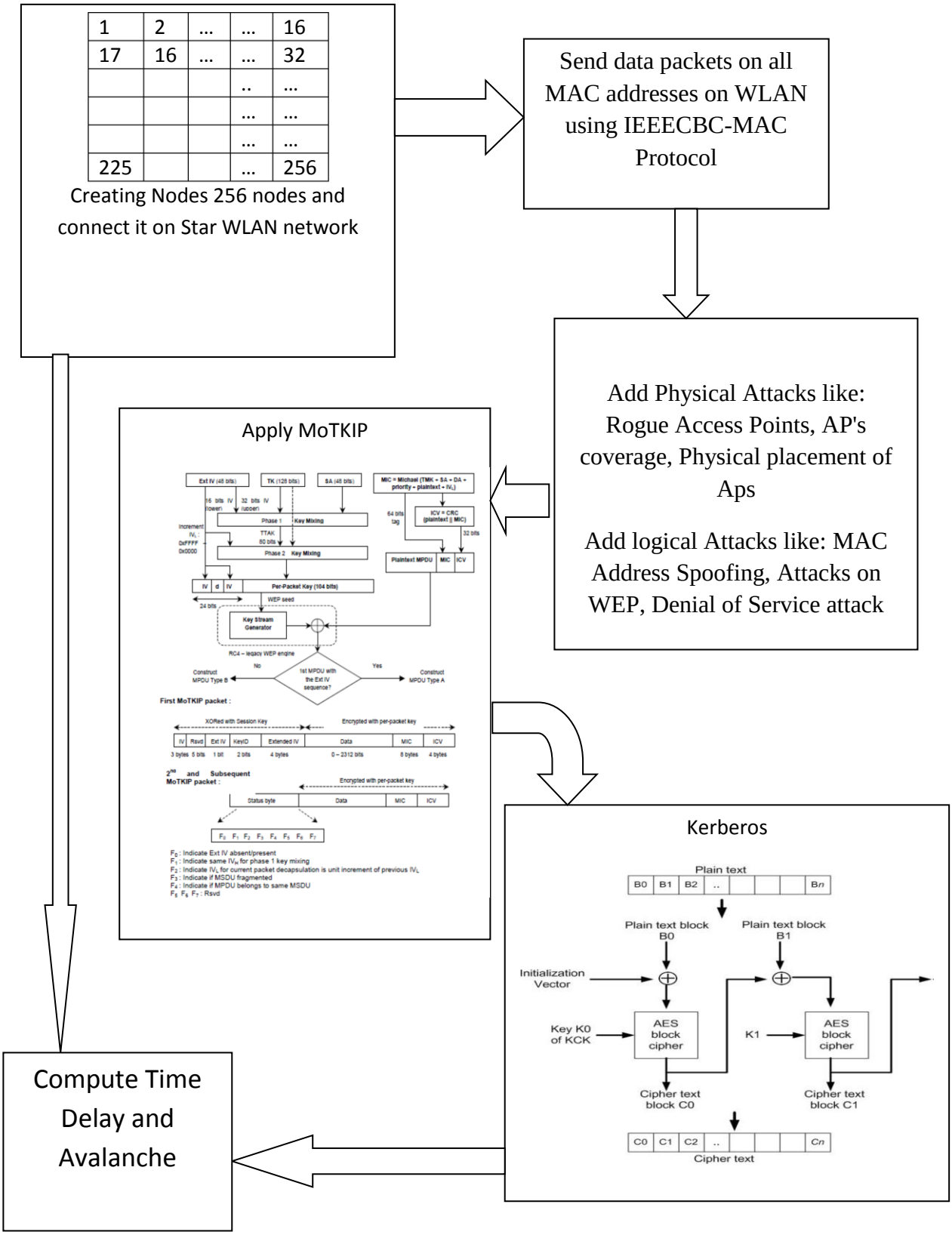


Figure 3 Proposed Flow diagram of WLAN security

4. RESULTS

The experimental test setup used an access point and 802.11b wireless network cards to establish and test secure communication performance. 11 Mbps was the nominal data rate. Clients transfer encrypted files to the server. The server looks for the status byte header on each data packet it receives to determine the appropriate MoTKIP algorithm for decryption. In order to confirm the MoTKIP operation and WLAN performance throughput, a number of statistical experiments were carried out. We will discuss each and every outcome of our TKIP work in this section.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 03, March 2023, pp : 123-130

e-ISSN : 2583-1062

Impact Factor : 5.725

Parameters: Time to execution, throughput, and total avalanche are TKIP work parameters.

Time delay: It is time taken to developing output cipher from input data.

Throughput: It is rate to generating cipher per seconds may be compute from formula below

$$\text{throughput} = \frac{\text{No. to Bits}}{\text{Time taken}}$$

Avalanche: It is total number to bits change between output ciphers before and after single bits change in key & it may be describe by formula below [15]

$$\text{Avalanche} = (\text{Cipher}_{\text{key}}) \text{ XOR } (\text{Cipher}_{\text{key+1}})$$

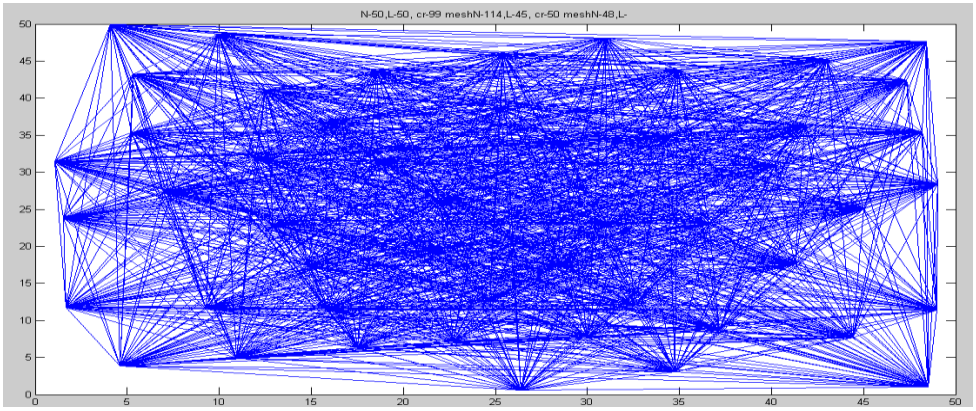


Figure 4 Mesh connections of nodes in the network

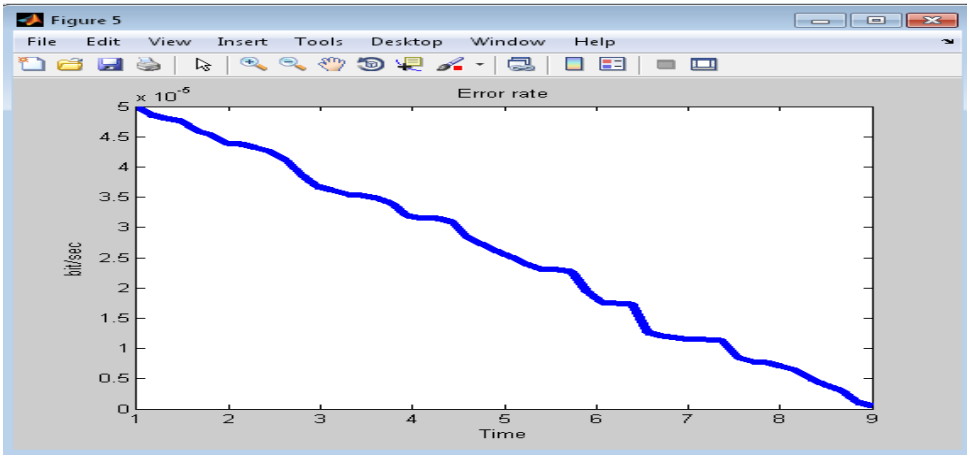


Figure 5 Error Rate Obtain for the proposed work for different time slots

From Avalanche Simulation to Test: Avalanche was observed with three different data inputs: Test 1: The text of the first test cipher is "EA324AED32E20179," and if we develop a cipher using the same data and a single bit of key change, the new key is "0123456789ABCDEE," and the new cipher is "1D08632DE5B6017C," with a total change of 70 bits between the new and old ciphers.

Test2: The text of the second test cipher is "28510AB4CDE97EA2," and if we develop a cipher using the same data and a single bit of key change, the new key is "FEDCBA9876543211," and the new cipher is "3A4C9F7AE297D802," with a total change of 69 bits between the new and old ciphers.

Test3: The text of the third test cipher is "D3D8E2290EACF41A." If we develop a new cipher using the same data and a single bit of key change, the new key is "FEDCBA9876543211," and the new cipher is "B4C982A8C4D5D5E8." The total change between the new and old cipher is 73 bits. From table 1 On behalf to above results we may conclude that minimum Avalanche to TKIP work is 72.

TABLE 1 Avalanche Observed For Proposed Tkip Cum Kerberos Work

SN	Test	Avalanche observed
1	Test-1	75
2	Test-2	72
3	Test-3	77

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 03, March 2023, pp : 123-130

e-ISSN : 2583-1062

Impact Factor : 5.725

Time Test to Simulation: time delay is been observed to three various data input shown in table 2, On behalf to above results we may conclude that maximum time delay is 0.928 seconds to TKIP work.

Table 2 Time Delay Observed For Proposed Tkip Cum Kerberos Work

SN	Test	Time delay observed
1	Test-1	0.919
2	Test-2	0.928
3	Test-3	0.913

Throughput Test to Simulation: Throughput is been observed to three various data input show in table 3, On behalf to above results we may conclude that minimum throughput is 137.931 kbps to TKIP work.

Table 3 Throughput Observed For Proposed Tkip Cum Kerberos Work

SN	Test	Throughput observed
1	Test-1	139.2828
2	Test-2	137.931
3	Test3	140.1972

Comparative results: Comparative results are been developed to compare TKIP work with available works here we have compared our work with latest & related work

Table 4 Comparative Results

	Time delay in second	Avalanche in db
Proposed MoTKIP Cum Kerberos work	0.928	72
Kerberos by Yi Ma [1]	3.45	69

Comparative results above show that as compare with work Kerberos [1] our work is similar in security because avalanche observed in TKIP work is same, however time delay by Kerberos is almost 300% much than our work which makes TKIP work faster than their work. As compare with others two works [2], [3] TKIP with is better in all parameters avalanche, throughput & time delay.

Table 5 Comparative Results Average Traffic

	Average Traffic (packets/sec)		
Time (ms)	EAP TLS [2]	KEAP [1]	Proposed Kerberos with TKIP
1	0.225	0.295	0.111
3	0.339	0.436	0.4925
5	0.452	0.603	0.9277
7	0.502	0.698	1.301
9	0.543	0.73	1.9583

Table 6 Comparative Results Average Bit Rate

Average Bit Rate (bit/sec)			
Time (ms)	EAP TLS [2]	KEAP[1]	Proposed Kerberos with TKIP
1	0.0005	0.00038	0.0001969
2	0.00039	0.000232	0.00015
3	0.00034	0.000164	0.0001221
4	0.00029	0.000131	0.000112
5	0.000275	0.000119	0.0001051
6	0.000243	0.000115	0.0000971
7	0.00024	0.000112	0.0000816

8	0.000228	0.000113	0.0000616
9	0.000227	0.000137	0.0000025

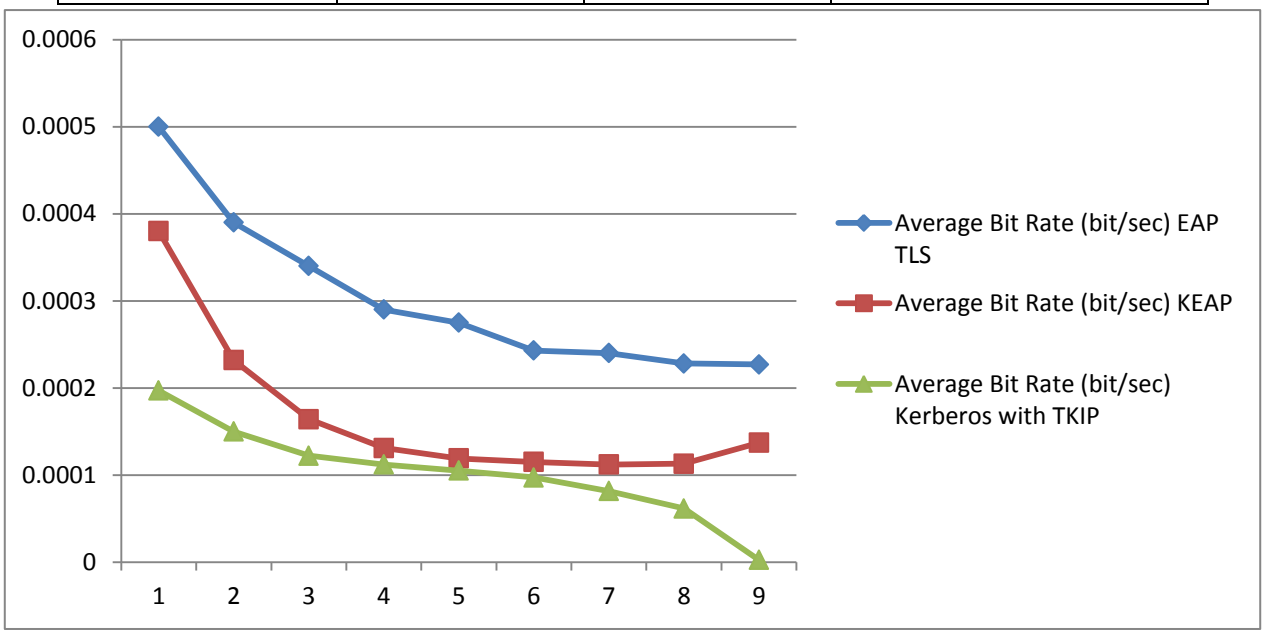


Figure 6 Comparison of Average bit rate

According to table 6, the proposed work has the highest average traffic for the same number of nodes, and according to figure 6, the proposed work has the lowest average bit error, indicating that more accurate data is being received at the receiver end.

5. CONCLUSION

IEEE802.11 was initially developed to connect wired networks and wireless devices. the point was to accomplish organizing with least or no security. At that point, security was not a big deal. However, with the success of WLANs and the rapid adoption of this technology, security became a big deal, and getting security right became a big concern. The Advanced Encryption Standard (AES) is a new standard that addresses new security protocols and introduces the strong block encryption algorithm. It also introduces a new key management scheme. IEEE802.11i can stop attacks on authentication, integrity, and privacy. In terms of logical attacks, IEEE802.11i offers sufficient defenses against WEP flaws, man-in-the-middle attacks, forgery packet attacks, and replay attacks.

6. REFERENCES

[1] The Improvement of Wireless LAN Security Authentication Mechanism Based on Kerberos, Yi Ma and Hongyun Ning, 2018 International Conference on Electronics Technology, 978-1-5386-5752-2/18/IEEE

[2] Abhijit Bodhe Mayur Masuti Dr. A.S.Umesh, wireless lan security attacks and ccm protocol with some best practices in deployment of services, 2395-0056 quantity: 03 issue: 01 january 2016

[3] Emil selvan gsr, gayathri n, rakesh kumar s, ankush rai, jagadeesh kannan r, advanced encryption and extended authentication for wireless local area networks, Advances in Smart Computing and Bioinformatics, Special Issue (Apri-2020)

[4] Matthew S. Gast, 802.11 Wireless Networks, O'REILLY, 2002, http://dx.doi.org/10.22159/ajpcr.2017.v10s1.19987.

[5] Cryptography and Network Security, Principles and Practices, Third Edition, Prentice Hall, 2003, by William Stallings.

[6] "Implementing Improved WLAN security," presented at the 46th International Symposium on Electronics in the Marine, by Matija Sorman, Tomislav Kovac, and Damir Maurovic. Zadar, 2004 ELMAR Croatia, June 16-18, 2004

[7] Derrick Dicoi and Joon S.Park, "WLAN Security: "Now and in the Future." Oct. 2003, IEEE Computer Society

[8] Gary McGraw and Nancy R. Mead. The Future of Wireless Security." IEEE Security and Privacy, August 2003, IEEE Computer Society.

[9] "Providing for Wireless LAN Security, Part 2," by Joseph Williams. November and December 2002 issues of IEEE IT Pro.

[10] "Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications," ANSI/IEEE Std. 802.11, 1999 Edition (R2003), is the IEEE standard for local and metropolitan area networks.

[11] Shin, M.; Ma, J.; A. Mishra; Arbaugh, W.A., "Remote organization security and interworking", Procedures of IEEE, Volume 94, Issue 2, pp 455 - 466, February 2006.

[12] "Wireless LAN and its security problem," by ZhangJi, Wang Shunman, TaoRan, and WmgYue. The Fourth International Conference on Parallel and Distributed Computing, Applications, and Technologies, 2003, was published in its proceedings. PDCAT'2003.