THINK INDIA JOURNAL

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

Enhanced security of WEP Using RSA against Dictionary attacks

Dhiraj Kapila
dhiraj.23509@lpu.co.in
Computer Science and Engineering
Lovely Professional University
Phagwara, India

Harwant Singh Arri
hs.arri@lpu.co.in
Computer Science and Engineering
Lovely Professional University
Phagwara, India

ABSTRACT

Wired equivalent privacy is a deplored procedure to shelter IEEE 802.11 wireless networks. The wireless networks transmit packet data by with the help of radio and hence the wireless networks have much prone to spying than wired networks. Wired equivalent privacy was envisioned to deliver secrecy analogous to outmoded wired network. During the initial days of 2001, the researchers performed the cryptanalysis procedure and originates some thoughtful faintness with the outcome that nowadays a wired equivalent privacy construction can be chopped or hacked with willingly accessible programs within sixty seconds. The IEEE society of engineers formed a novel 802.11i working group within a short period of time to counter the issues related to WEP security. WEP possess secrecy by employing torrent cipher RC4 and possess truthfulness by employing the CRC-32 checksum. Wired equivalent privacy formulates a key plan as a fragment of encryption procedure, by merging arbitrarily created twenty-four-bit initialization vector (IV) through the common private key specified by the handler of the communicating station. This was revealed lately that the decryption of RC4 cipher text is very informal as wired equivalent privacy initialization vectors are spread in clear. The aim of given research paper is the scrutinize the routine of wired equivalent privacy by implementing extra protect encryption algorithm rather to employ RC4 method. It has well identified that RC4 cipher text has one frail key available from every two fifty-six keys. The frails keys can be circumvented. We have proposed the new RSA procedure by substituting RC4 and CRC32 procedure in WEP structure. Here we pretend the WEP structure by employing network simulator2 with dictionary assaults.

Keywords

Initialization vector, RC4, CRC32, MD5, RSA, WEP, Checksum , Key management, Rivest Cipher and Dictionary attack.

1. INTRODUCTION

Wireless Local Area Network commonly known as WLAN which is operated as Wi-fi, Wi-MAX. WLANs are a packet broadcasting scheme intended to deliver site driven self-governing network admittance among various communicating devices with the usage of radio waves as an alternative to wired or cable type network structure. In the year of 1997, the 802.11 description as a specification was accepted by the Institute of Electrical and Electronics Engineers (IEEE) for wireless local area networks. Comparable to all other IEEE 802 standard specifications, the 802.11 standard emphasis on the two popular nethermost layers physical and data link of open system interconnection model. Wireless local area networks are typically introduced in the commercial businesses as the closing connection among the existing cable type local network and a group of user systems, providing such users a wireless contact to the use complete resources and facilities of the business network within the company building, room or campus. The chief inspiration and advantage from wireless local area networks is amplified mobility. Contrasting to conformist network connections, wireless local network patrons can relocate practically deprived of constraint and contact local area networks approximately from anyplace.

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

Other reimbursements for wireless local area networks comprise price productive network deployment for the locations such as longstanding structures and rock-hard vertical brick or stone structures where the installation of cable type network is not possible. The usage of WLANs abridged proprietorship costs, predominantly in active surroundings requires continuous fluctuations because of its negligible cable and connection price per customer.

Wireless local area networks make users free from the necessity on solid wired contact to network support. A WLANs practices radio waves in the same way alike mobile phones, TVs and transistors uses. Indeed, wireless packet transmission is similar as dual way radio communiqué. In this dual way radio transmission, a system's wireless connector deciphers information into radio waves and then communicates data with the help of antenna which is a device to receive radio waves or signals. The decoding of received radios wave signals by a special device cableless router. The wireless router transmit packet information over the web by means of a physical or cable type local area network connection. The procedure as well performed in converse, through the wireless router obtaining data packets from the web, interpreting the accepted data in the form of radio waves and broadcast the data to the system's wireless connecter. The signal's employed for wireless fidelity communiqué are identical to the radio signals employed for ipads, tablets, walkie-talkies, mobile phones and other similar wireless communicating equipment's. These equipment's could communicate and accept radio signals and then translates the binary information into radio signals and change the radio signals back into binary information. If passably secured, an unofficial handlers or illegal person who practice the link as a free web linking could easily avail the facility a wireless fidelity network. The action of tracing and manipulating security uncovered wireless local networks are known as warbiking. An recognizing a standard iconography commonly referred as "Warchalking", has progressed. Cabletype o cableless local area networks approximately shares similar security threats such as physical layer security threat, group participant attacks, illegal contact, hacking and snooping. During late in the year 2001,a research is issued from the wireless fidelity alliance which reveals that "security threats has already the intervening apprehension concerning wireless networking placement" [WECA, 2001b], amid seventy two percent of wireless anticipator's and fifty percent of wireless adapters'. A nomenclature of security intimidations is represented in Figure 1. The presented security attacks could originate from core or outside sources available.

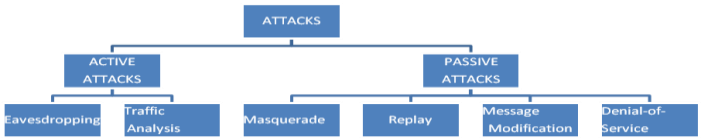

Fig 1: Taxonomy of Security Threats

1.1 Passive Attacks

An unofficial group increases admission to a wireless local area network and but the attacker could not able to change the resources on the local area network. Categories of passive attack include:

- Snooping: An invader merely observes and eavesdrops to information broadcasting. For example, an unofficial user walks through the metropolitan city and eavesdrops to different wireless local area network communications inside diverse organizations (i.e. warbiking,).
- Network Traffic Investigation: An invader screens the wireless network traffic for transmission outline examination. The information composed could be practice to accomplish a dictionary attack.

1.2 Active Attacks

An unofficial group increases admission to a wireless local area network and amends the different wireless local area networks resources easily. An invader first gets the access of media access control address or the internet protocol address of a

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

handler/device to increase network admittance, and then transform the given info of the wireless area network resources.

Various kinds of active attack comprise:

- ***Masquerading:*** An invader copies a privileged handler and thus increases some mentioned unsanctioned operating rights. Masquerading comprises the practice of hoaxing, reprobate APs, and resending assaults. An invader could dupe handlers to switch on to the reprobate AP by introduction a reprobate AP in the similar domain as an effective AP, transferring the similar SSID by using a sound signal than the lawful AP. The invader is capable to interpret the public key from the traffic composed from the network. The reprobate AP can be employed to transmit handler communications to an illegal end point enclosing de-authentication data.
- ***Replay:*** An invader observes the network rush (passive attack) and then resends the information as the authentic handler.
- ***Message Modification:*** An invader modifies the authentic information by removing, inserting, modifying, or resaving it. Apart from that, an invader can amend the specification of known equipment, such as, ***simple network management protocol*** **(SNMP**) to constitute access points.
- ***Denial-of-service*** **(DoS):** An invader avoids or concentrates the standard practice or supervision of wireless local area network systems impractical by delivering malevolent instructions or inserting a huge volume of network rush which blocks up up the wireless rate of recurrence. The above said passive attack could be expand moreover to ***distributed DoS (DDoS)*** assaults.

Hence any unit that encompass the WLANs must employ security precautions for example, wired equivalent privacy (WEP) encoding method, the added wireless fidelity safety admittance (WPA), Web Protocol Safety(WPS), or a cybernetic isolated network (CIN).

2. Wired Equivalent Privacy (WEP)

Wired equivalent privacy is a deplored procedure to protect IEEE 802.11 wireless local area networks (WLANs). Wireless local area networks (WLANs) transmit information by means of radio waves and hence much liable to spying than cabletype local area networks.

During the announcement of WEP in the year 1997, wireless equivalent privacy was envisioned to deliver privacy analogous to that of old-style cabletype local area network. Starting in 2001, cryptanalysts recognized numerous thoughtful faintness with the outcome that a wireless equivalent privacy linking can nowadays be hacked within a quick duration with voluntarily accessible software's. The IEEE society of engineers created a novel 802.11i unit group within a limited month to combat the issues. In the beginning of year 2003, the wireless fidelity coalition communicated to the world that wireless equivalent privacy was substituted in wireless fidelity secured admittance, a variant of the anticipated update to 802.11i. Lastly, in the end of year 2004, with the endorsement of the complete 802.11i standard (i.e. WPA2), the IEEE society of engineers acknowledged that together wireless equivalent privacy version 40 and wireless equivalent privacy version 104 "were denounced as the IEEE society unsuccessful to accomplish the archived safety objectives." Regardless of its shortcomings, wireless equivalent privacy is still commonly used approach. WEP is habitually the prime security option recommended to handlers by wireless router specification resources which offers a highest layer of safety that daunts lone inadvertent usage, parting the local area network susceptible to cautious conciliation .Wireless equivalent privacy was encompassed as the confidentiality of the initial IEEE 802.11 standard sanctioned in the month of September of the year 1999. Wireless equivalent privacy employs the torrent cipher RC4 aimed at

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

secrecy, and available CRC-32 error checksum for truthfulness. This was deplored as a wireless privacy method in the year of 2004, but for bequest drives till now is recognized in the existing standard. Wired equivalent privacy formulates a key plan as a fragment of encryption procedure, by merging a arbitrarily created twenty four bit initialization vector (IV) through the common private key specified by the handler of the communicating station. The initialization vector elongates the lifespan of the private key since the place can alter the initialization vector for every frame broadcast. Wired equivalent privacy contributes the subsequent "seed" on a deterministic random bit's producers who generates a key flow equivalent to the span of the frame's actual includes a integrity check value of size thirty two bits.

The integrity check value is a datum employed for detecting error that the packet reception place ultimately re-evaluates and relates to the individual transmit by the transferring place to judge whether the communicated information undertook any method of interfering while not transient. If the reception place estimates an integrity check value that never equals the individual originate in the data frame, then the receipt place can castoff the data frame or ensign the handler.

Wired equivalent privacy stipulates a common private key of 32 or 64 bit to encode and decode the information. Few companies in addition provides secret keys of 128 bits for later version of wired equivalent privacy (WEP) known as "WEP2.0" in the manufactured items. The receipt station will have to practice the same private key for decoding with WEP. Wired equivalent privacy integrates the key flow with the meta-data /integrity check value by a bitwise XOR structure before the broadcast held which generates the encrypted text. Wired equivalent privacy embraces the initialization vector inside the transparent within the initial group of bits of the data frame. The receipt place practices that initialization vector along with the common private key provided by the handler of the receipt place to decode the meta-data part of the data frames. Dual approaches of authentication could be employed with Wired equivalent privacy. The first approach is OSA and other approach is SKA. The OSA approach is known as open system authentication while SKA is shared key authentication. In OSA approach, the wireless local area network does not require to give its authorizations to the APs throughout the substantiation process. Hence, any user, irrespective of its wired equivalent privacy keys, can substantiate himself through the APs and then try to subordinate. As a consequence, not at all substantiation happens.

Wired equivalent privacy can be implemented to encode the data frames after substantiation and affiliation. The users should have the correct key stream at this stage. In the SKA approach, wired equivalent privacy is employed for confirmation. During the usage of SKA approach a quadruple part contest reply handclasp is used:

1. The patron place transmits a verification appeal to the wireless AP.
2. The AP transmit back an apparent manuscript contest.
3. The patron has to encode the contest manuscript by means of the constructed wired equivalent privacy key, and then transmits it back to alternative verification appeal.
4. The AP decodes the substantial, and associates it with the apparent text an AP had transmit. Reliant on the achievement of this contrast, the AP transmits in return a optimistic or undesirable reply.

After the linking and verification, wired equivalent privacy key could be employed for encoding the packet data. However, wired equivalent privacy has experienced considerable inspection and reproach since many years. wired equivalent privacy has directed a anxious reality because of numerous safety threats. These safety threats comprise of:

1. The huge fraction of wireless local area networks (WLANs) have wireless equivalent privacy

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

deactivated due to directorial overhead of preserving a common wired equivalent privacy key.

2. Wired equivalent privacy has the similar issue as the entire systems depends on common keys: any privacy apprehended by individual or many users quickly turn out to be open knowledge. For example, an operative who has just left his company still remembers the common wired equivalent privacy key. This previous operative could be seated himself at external side of the company premises with an 802.11 network interface card and snuffle network rush or even hack the inner local area network.
3. The IV that kernels the wired equivalent privacy process is directed in the vibrant.
4. The wired equivalent privacy error detection process is rectilinear and probable.

3. WIRED EQUIVALENT PRIVACY PROCEDURE

Wired equivalent privacy frame representation as follows

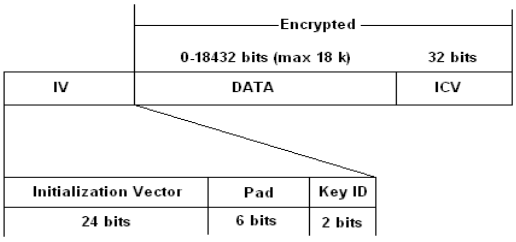

Fig 2: WEP Data Format

As predicted by Songhe Zhao and Charles A. Shoniregun [5], the private key employed in wired equivalent privacy procedure is 5 bytes lengthy with a 3 bytes initialization vector (IV) that is conjugated for substitute as the encoding/decoding key. The resultant key turns as the kernel for a pseudo random number generator (PRNG). To attain the encrypted text, the pseudo random number generator practices the RC4 method to generated a pseudo-random bit classification that further XOR through the normal text.

The wired equivalent privacy encoding procedure starts as follows.

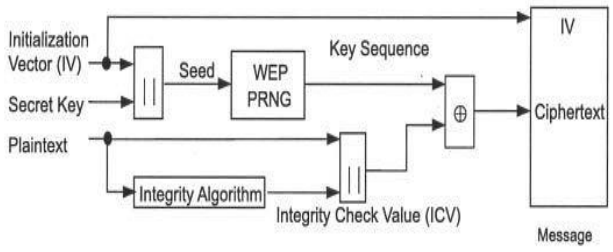

Fig 3: WEP encryption

There are dual procedures functional to the WEP encoding. First evaluates a thirty-two-bit integrity check value (IVC) by employing CRC-32 procedure on the whole message normal text to defend in contradiction of illegal information alteration. Another procedure i.e. encoding of normal text, the private key is conjugated with an initialization vector resultant in a sixty-four-bit entire key extent. The initialization vector elongates the lifespan of the private key since the place can alter the initialization vector for every data communication [8]. Wired equivalent privacy contributes the resultant key, commonly refereed as 'seed', inside the pseudo random number generator that vintages a key classification equivalent to the span of the normal text plus the integrity check value. The resultant classification is employed to encode the lengthened normal text by undertaking a function of bitwise XOR. A concluding encoded information is finished by ascribing the initialization vector in obverse of the cryptographic text. If WEP comprise the 128-bit secret key, the solitary variance is that the clandestine key extent turns out to be 104 bits and the initialization vector relics 24 bits.

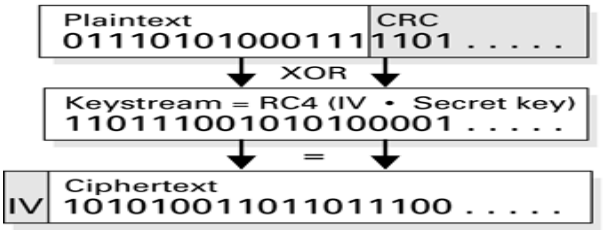

Fig 4: Encrypted WEP Frame

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

Initialization Vector (IV) of the inward text is employed to produce the key classification essential to decode the inward text for wired equivalent privacy. The cryptographic text, merged with the correct key classification, produces the unique normal text and integrity check value. The decoding is proved by executing the CRC-32 procedure on the improved normal text and associating the obtained integrity check value with the that integrity check value broadcast with the communication. If obtained integrity check value is not equivalent to broadcast integrity check value, the accepted text has a fault and further a signal is sent vertebral to the conveyance place.

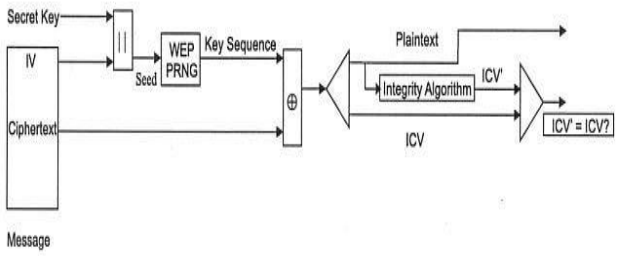

Fig 5 : WEP decryption

3.1 Issues with Wired Equivalent Privacy

Overall, raising the key volume raising the protection of an encryption procedure. Investigation study has revealed that key volume of larger than 10 bytes makes the Brute Force method tremendously problematic to apply in the encryption process. Wired equivalent privacy method of encryption is weak to few attacks irrespective of its key volume [5]. Even though the procedure of wired equivalent privacy may breaks the unplanned sniffers, strong-minded attackers could break wired equivalent privacy keys in a demanding local area network inside a moderately petite duration of time. In the above said part, we recapitulate fours chief security failings, that can be main origin the assaults.

3.2 Issue with initialization vector IV

Irrespective of the key volume, 24-bit length of wired equivalent privacy initialization vector could deliver "16,777,216" dissimilar RC4 cipher key flows for a specified wired equivalent privacy key. On a demanding wireless local area network, the following figure can be attained within short period of time and reprocess of the similar initialization vector further turn out to be inevitable. RC4 cryptogram key flow uses bitwise XOR and combines with the unique message to produce the encoded data that is communicated, and the initialization vector is directed in the apparent with every message. If an attacker accumulates adequate data frames founded on the similar initialization vector, the user can control the common standards between them, for example, the key flow or the common private key. Since preforming the bitwise XOR of dual cryptographic messages that employs the equivalent key flow would lead to cancellation of key flow and the outcome will the bitwise XOR of the dual normal texts. When the dual encoded data frames which possesses the similar initialization vector are revealed, different approaches of assault can be functional to convalesce the normal. This theory is clarified by subsequent evaluations

C1 = Cryptographic message 1

C2 = Cryptographic message 2

N1 = Normal text 1

N2 = Normal text 2

IV = Initialization Vector

S = Secret Key

X = bitwise XOR

If C1=N1 × RC4(IV,S) & C2=N2 × RC4(IV,S)

Then

C1XC2 = (N1 X RC4(IV,S)) X (N2 X RC4(IV,S))

= N1 X N2

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

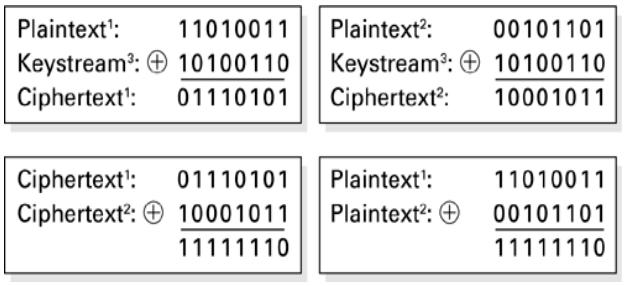

Fig 7: Key Stream Attack

The above-mentioned examples reveal that the XOR outcome of normal texts and the XOR outcome of normal texts is identical while by means of the similar key flow. Hence, if the hacker identifies a normal text when initialization vector is reprocessed, he may recognize another normal text even the hacker does not remember any key flow.

3.3 Key Administration is Underprivileged

The 802.11 specification document does not postulate how the supply of keys would be achieved. Without interpretational key administration, keys would incline to be long-lasting and deprived eminence. Many cableless local area networks that employs wired equivalent privacy has unique sole wired equivalent privacy key common among each system node on the local area network. APs and handler places should be embedded with the identical wired equivalent privacy key. Meanwhile coordinating the alteration of keys is monotonous and problematic, wireless local area network superintendents should individually call every wireless equipment in practice and physically insert the suitable wired equivalent privacy key. Following process might be be adequate at the connection phase of a wireless local area network or when a novel user switch on the wireless local area network system, but whenever the key turns out to be negotiated or there may be harm to safety or security, the key should be transformed. The following process might not be an enormous matter of concern in a tiny company consisting limited clients, but the process could be unrealistic in big organizations, which characteristically have thousands of clients. As a significance, possibly thousands of clients and equipment can be be consuming the similar key for large duration of time. Every WLANs rush from every client would be encoded by means the similar key; that made it simplify for somebody eavesdropping to network rush to break the keyframe, since bulk data messages are being communicated by means of similar key. In preparation, maximum connections employ a solitary key for a whole local area network. This exercise extremely influences the safety of the structure, since a private that is public amid many clients could not store very skillful concealed.

3.4 The CRC-32 checksum is unsuitable

The wired equivalent privacy integrity check value is grounded on CRC-32 checksum, a process for noticing sound and shared errors in communication. “CRC-32 checksum” is an exceptional checksum method for spotting errors, but an dreadful option for a encrypted mess. The integrity check attribute is instigated like a “CRC-32 checksum,” which is part of the translated metadata of the message. Nevertheless, “CRC-32 checksum is rectilinear, which describes that it is conceivable to calculate the bit alteration of dual CRCs grounded on the big change of the packets on which the packets are engaged. In similar term, flicking bit N in the packet’s fallouts in a settled sequence of bits in CRC that should be spun to generate an accurate checksum on the adapted information. Since flicking bits transmits by and afterward an RC4 decoding, this permits the hacker to dismissive random bits in an encoded data and appropriately regulate the checksum hence the subsequent communication may give the impression as allowed communication.

3.5 Easy counterfeiting of verification messages

802.11 specification announced dual categories of verification; OSA and SKA. The hypothetical impression was that a verification would be healthier option than none authorization. But in realism, the contradictory is appeared to be factual. Rotary on substantiation with wired equivalent key, actually

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

diminish the over-all protection of the wireless local area network and made it simply to wired equivalent key for the hackers and invaders. SKA representing the acquaintance of the common WEP key by encoding a test. The issue occurred here is, screening assailant could detect the task and the scrambled the given reply. Due to this, an assailant could regulate the RC4 key flow employed to encode the answer, and employ that flow to encode any task he/she might accept in the forthcoming. Hence by screening a positive authorization, the assailant in future can falsify an substantiation. The solitary gain of SKA is that this type of authentication diminishes the capability of an assailant to form a DoS assault by transferring junk messages inside the wireless network.

4. INTENDED ALGORITHM

Experimental investigation had discovered that RSA has abundant protection as equated with RC4 procedure. The given fallouts are self-possessed structure of the wired equivalent privacy for RSA with message digest five hashing approach. This is examined that the output of safety procedure is continuous as is specified by the single lines. And there is negligible harm in the data frames. We have intended the duration for the diverse nodes in experimental study.

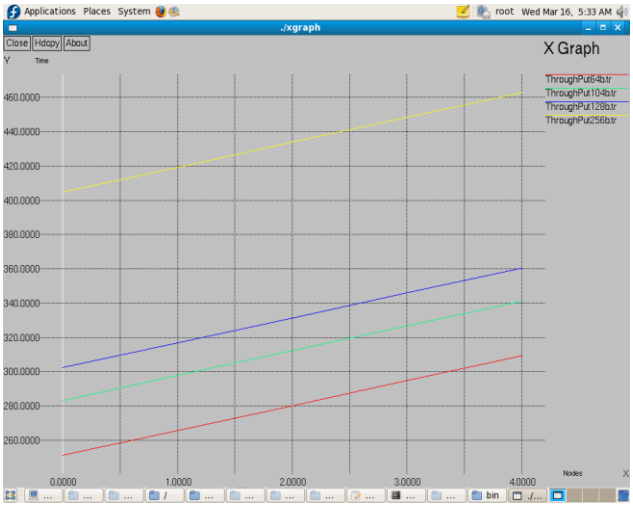

Fig 6: Comparisons between RSA and RC4

5. CONCLUSION

The above experimental study has determined that there is negligible variations in the time feeding as contrast with “Rivest Cipher 4” stream cypher and “CRC 32 checksum”. This investigation presented above might be applied in empathetic the safety or protection of the wireless local area network to large scope so as to deploy the WLANs with highly secure and hacking free.

6. REFERENCES

[1] Reddy, S.V. Sai Ramani, K. Rijutha, K. Ali, S.M. Reddy, “ Wireless hacking - a WiFi hack by cracking WEP” , IEEE, vol. 1, pp. V1-189 - V1-193, 22-24 June 2010.

[2] Kai Zeng, Kannan Govindan, and Prasant Mohapatra, “Non-cryptographic authentication and identification in wireless networks” , IEEE, Wireless Communications, vol. 17 , Iss. 5 ,pp. 56 – 62, October 2010 .

[3] Yao Yao Jiang Chong Wang Xingwei, “Enhancing RC4 algorithm for WLAN WEP protocol “ ,IEEE, Control and Decision Conference , pp. 3623 – 3627, 26-28 May 2010.

[4] Ming Li Wenjing Lou Kui Ren, “Data security and privacy in wireless body area networks” , IEEE , Journals, Wireless Communications, vol. 17, pp. 51 – 58 ,18 February 2010.

[5] Zhang Longjun Zou Tao, “An Improved Key Management Scheme for WEP” ,IEEE, International conference on Embedded and Ubiquitous Computing, pp. 234 – 239, 17-20 Dec. 2008.

[6] Zhao, Songhe and Shoniregun, Charles,“Critical Review of Unsecured WEP” , IEEE, Conference ,pp. 368 - 374 ,9-13 July 2007

ISSN: 0971-1260

Vol-22-Issue-17-September-2019

[7] Security" ,IEEE , Workshop on High Performance Switching and Routing 2005,pp. 376 –380,12-14 May 2005 Date of Current Version: 06 September 2005.

[8] S.Chandramathi,K.V.Arunkumar, S.Deivarayan and P.Sendhilkumar, "Fuzzy based Dynamic WEP keymanagement for WLAN Security Enhancement" ,IEEE ,Workshops on Communication Systems Software and Middleware, 3rd International Conference ,pp. 409 – 414, 27 June 2008.

[9] Reddy, S.V. Sai Ramani, K. Rijutha, K. Ali, S.M. Reddy, "Wireless hacking - a WiFi hack by cracking WEP" , IEEE, Education Technology and Computer 2nd International Conference, vol. 1, pp. V1-189 - V1-193, 22-24 June 2010.

[10] Hole, K.J. Dyrnes, E. Thorsheim, "Securing Wi-Fi networks". , IEEE Journals , Computer, vol.38 , pp. 28 – 34,July 2005.

[11] S. Chandramathi,K.V.Arunkumar,S.Deivarayan, P. Sendhil Kumar, K.Vaithiyanathan," Modified WEP key management for enhancing WLAN security", IEEE , International Journal of Information and Communication Technology ,vol.1,pp. 437 - 452,2008.

[12] Lashkari, Arash and Towhidi, Farzan, "Wired Equivalent Privacy", IEEE, Future Computer and Communication, International Conference, pp. 492 – 495, 3-5 April 2009.

[13] S.Chandramathi,K.V.Arunkumar, S.Deivarayan and P.Sendhilkumar, "Fuzzy based Dynamic WEP keymanagement for WLAN Security Enhancement" ,IEEE ,Workshops on Communication Systems Software and Middleware, 3rd International Conference ,pp. 409 – 414, 27 June 2008.

[14] Zhao, Songhe and Shoniregun, Charles, "Critical Review of Unsecured WEP" , IEEE, Conference ,pp. 368 - 374 ,9-13 July 2007 .

[15] Bittau, Handley and Lackey, "The Final Nail in WEP's Coffin" , IEEE , Security and Privacy, pp.15 – 400, 21-24 May 2006.

[16] Matija Sorman, Tomislav Kovac, Damir Maurovic, "Implementing improved WLAN Security" ,IEEE ,Proceedings Elmar 2004, 46th International Symposium, pp. 229 – 234,16-18 June 2004

[17] Majstor, F, "WLAN security threats & solutions" ,IEEE, Local Computer Networks, Proceedings 28th Annual IEEE International Conference, pp. 650, 20-24 Oct. 2003.

[18] Hani Ragab Hassan, Yacine Challal,"Enhanced WEP: An efficient solution to WEP threats" , IEEE , Wireless and Optical Communications Networks, 2005. Second IFIP International Conference , pp. 594 – 599, 6-8, March 2005 .

[19] Zeynep Gurkas, A. Halim Zaim, M. Ali Aydin, "Security Mechanisms and their Performance Impacts on Wireless Local area Network", IEEE , Computer Networks, International Symposium 2006,pp. 1 – 5,31 July 2006.

[20] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems.