International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319 – 6505, Impact Factor: SJIF: 5.995
Available Online at www.journalijcar.org
Volume 6; Issue 7; July 2017; Page No. 4640-4645
DOI: http://dx.doi.org/10.24327/ijcar.2017.4645.0549

Research Article

AN IMPROVED MECHANISM FOR FOUR-WAY HANDSHAKE PROCEDURE IN IEEE802.11w

Sourabh patel and Hariom soni

Department Of CSE IMEC, Sagar (M.P.)

ARTICLE INFO

Article History:

Received 22nd April, 2017
Received in revised form 10th May, 2017
Accepted 13th June, 2017
Published online 28th July, 2017

Key words:

Wi-Fi, WEP, ICV, WPA, TKIP, MIC, MAC, RSNA.

ABSTRACT

As the acceptance and popularity of wireless networking technologies has proliferated, the security of the IEEE 802.11 wireless local area network (WLAN) has advanced in leaps and bounds. From tenuous beginnings, where the only safe way to deploy a WLAN was to assume it was hostile and employ higher- layer information security controls, to the current state of the art, all manner of improvements have been conceived and many implemented. This work investigates some of the remaining issues surrounding IEEE 802.11 WLAN operation. While the inherent issues in WLAN deployments and the problems of the original Wired Equivalent Privacy (WEP) provisions are well known and widely documented, there still exist a number of unresolved security issues. These include the security of management and control frames and the data link layer protocols themselves. This research introduces a novel proposal to enhance security at the link layer of IEEE 802.11 WLANs and then conducts detailed theoretical and empirical investigation and analysis of the effects of such proposals.

INTRODUCTION

This paper explains the evolution of security for wireless networks. The paper provides a comparative study between three major security protocols: Wired Equivalent Privacy (WEP), Wi-fi Protected Access (WPA) and Wi-fi Protected Access 2 (WPA2). This research paper begins with a general introduction of four way handshaking, followed by the retrospect of 802.11w protocol evolution history and comparison with several related technologies. Through analyzing system architecture, deployment model and service type, the characteristics of 802.11 are concluded from technical, functional, security and economical aspects. After that, current efforts both from commercial and research perspectives are presented in order to capture challenges and opportunities in this domain. In the book of Enhanced Communication Security and Mobility Management in Small-Cell Networks, Suneth Namal mentions the role of four way handshaking within the technology world to be equal to the identification in the industrial age [2]. Today, organization uses their own security resources however with four way handshaking organization would merely request for the security resource from the organization maintaining such resources. This would lower the cost of maintaining large number and expensive machines, storage space etc. therefore the resource aren't any additional dedicated to only user or owner, however are being shared by multiple users at network level, host level and application level. Conjointly user got to purchase resources they use and also the time they need them. In four way handshaking tech. organization will request for as several resources they require and scale their resources to tens of thousands of system. The four way handshaking is helpful to organization as they currently got to focus solely on their target while not taking the headache of code change, hardware failure, system crash etc. Thus a straightforward definition of 4-way hand shake which relies on 5 attributes:

- ➢ Data Confidentiality and Integrity
- ➢ Mutual Authentication
- ➢ Data Availability

II Overview of IEEE802.11

- Single and unified solution needed for all IEEE 802.11 Protection-capable Management Frames.
- It uses the existing security mechanisms rather than creating new security scheme or new management frame format.
- It is an optional feature in 802.11 and is required for 802.11 implementations that support TKIP or CCMP.
- Its use is optional and can be negotiable between STAs.

Corresponding author:* **Sourabh patel
Department Of CSE IMEC, Sagar (M.P.)

Protected frame

Protection-capable management frames are those sent after key establishment that can be protected using existing protection key hierarchy in 802.11 and its amendments.
Only TKIP/AES frames are protected and WEP/open frames are not protected

- Disassociation and de-authentication
- Radio measurement action for infrastructure BSS (802.11k frames)
- QoS action frame (802.11e frames)
- Future 11v management frames (802.11v frames)
- Protection-capable Management Frames are protected by the same cipher suite as an ordinary data MPDU.
- MPDU payload is TKIP or CCMP encrypted.
- MPDU payload and header are TKIP or CCMP integrity protected.
- Protected frame subfield of frame control field is set.
- Only cipher suites already implemented required.
- Sender's pairwise temporal key (PTK) protects unicast management frame, and group temporal key (GTK) is used to protect broadcast/multicast management frame.
- A RSN (802.11i) IE capability bit used to signal whether Protection-capable Management frames are protected.

Replay protection

Replay protection is provided by already existing mechanisms. Specifically, there is a (per-station per-key per-priority) counter of each transmitted frame; this is used as a nonce/initialization vector (IV) in cryptographic encapsulation/de-capsulation, and the receiving station ensures that the received counter is increasing.

Usages

The 802.11w standard is implemented in Linux and BSD's as part of the 80211mac driver code base, which is used by several wireless driver interfaces; i.e., ath9k. The feature is easily enabled in most recent kernels and Linux OS's using these combinations. Openwork in particular provides an easy toggle as part of the base distribution. The feature has been implemented for the first time into Microsoft operating systems in Windows 8. This has caused a number of compatibility issues particularly with wireless access points that are not compatible with the standard. Rolling back the wireless adapter driver to one from Windows 7 usually fixes the issue. Wireless LANs send system management information in unprotected frames, which makes them vulnerable. This standard protects against network disruption caused by malicious systems that forge disassociation requests that appear to be sent by valid equipment.

III Wireless Networking Technologies

Wireless Networks utilize the infrared, radio or microwave spectra, under the governance of various protocol suites. Of these, commercial broadcast radio and television clearly had the greatest market penetration towards the end of the last millennium. However, now mobile phone ownership outstrips television ownership by almost 2:1 [12]. Besides the various mobile telephony protocols, which do not generally interfere with WLANs (other than for those MS that may dynamically switch between communications protocols, including the WLAN standards), some of the more common wireless networking technologies of relevance here are the Infrared Data Association (IrDA), IEEE 802.15 Bluetooth and Ultra wide band (UWB) personal area networks (PANs) and the IEEE 802.11 WLANs, all of which share various common spectra, along with a myriad of unrelated radiating devices.

IrDA

IrDA infrared links, using the near-infrared 5 (120-400 THz) spectrum, establish point-to-point connections at close ranges up to at least 1 meter, such as between two laptop devices or between a PDA and a printer or a mobile telephone, where such devices are IrDA capable. The IrDA inaccurately claims “the secure wireless link” [11] based on infrared being principally a line-of-sight transmission technology, thus limiting covert passive or active intrusion to those devices in the immediate vicinity. Relying on these short-range characteristics, IrDA provides no link level security and anyone within the unobstructed minimum 30° to maximum 60° [9] beam can monitor the transmission, including outside glass doors and windows and reflections from surfaces in rooms and vehicles.

Mobile Telephones

While mobile telephone handsets do not generally interfere with WLANs, most handsets today at least include Bluetooth capabilities and a few still provide IrDA capabilities, but more and more frequently these handsets are capable of operating over multiple network protocols. Those that are capable of utilizing Bluetooth or WLAN, when configured to swap between wireless network protocols, will regularly scan the air around them searching for the strongest or cheapest connection to use. This means regular probes in WLAN spectra if using active methods and added congestion whenever these spectra are chosen.

Bluetooth

Bluetooth is a short-range wire-replacement technology that implements a Wireless Personal Area Network (WPAN). It allows up to eight devices to connect together into a ‘piconet’. The most frequent use of Bluetooth technology has been for mobile telephones, not only as wireless headsets and hands-free use in cars, but also to synchronies configurations, data or even email with PDAs or PCs [7]. These uses are expanding to cable-free speakers in home theatre systems and Bluetooth headsets for personal stereos and MP3 players, although UWB also made a play for market-share on the former.

ZigBee

At the opposite end of the data-rate scale, IEEE Std 802.15.4 “ZigBee” (uses the ZigBee lightweight routing protocol) for telemetry and is designed for very low data rates, so as to give long battery life and low device cost. ZigBee operates in the 2.4 GHz ISM band by default, but uses 868 MHz in Europe and 915 MHz in the U.S. and Australia. IEEE Std 802.15.5, approved and publication expected April 2009, is planned to enable other WPAN meshes to be formed at the MAC layer, without needing ZigBee for routing.

WiMAX

In some remote communities, WLANs are deployed as the last-mile local loop by users lacking landline DSL or cable services. This has been a target market for the IEEE 802.16 [30] WiMAX Forum's broadband Wireless MAN protocol applications, which can also use the same spectra (although typically not) as WLANs.

IV Previous Work On IEEE 802.11 WLAN Protocols

The list of IEEE 802.11 amendments, updates and enhancements keeps expand- ing and has now circled the alphabet into double-character suffixes.

IEEE 802.11a, b, g and "Super G"

In 1997, the Institute of Electrical and Electronics Engineers published IEEE Std 802.11: Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) specifications [11]. This detailed requirements for frequency hopping WLANs in the 2.4 GHz band (2400–2483.5 MHz) [35]. In 1999, the International Organization for Standardization (ISO8) adopted ANSI/IEEE Std 802.11, 1999 Edition, as International Standard ISO/IEC 8802–11: 1999 [12].

IEEE 802.11a

In December 1999, the first amendment, IEEE Std 802.11a–1999 (International Standard ISO/IEC 8802–11:1999/Amd.1:2000 [7]), added specifications to pro- duce much higher data rates (6-54 Mbit/s) using orthogonal frequency division multiplexing (OFDM) in the 5.2 GHz band (5150–5350 MHz) and the 5.8 GHz band (5725–5825 MHz) [35]. Note that the 5.2 GHz band is directed at the USA-specific "unlicensed National Information Infrastructure (U-NII)" band, for which there is no equivalent purpose10 in the Australian Radiofrequency Spectrum Plan [8] (nor for many other countries outside the USA). The 5.8 GHz band (but not the 5.2 GHz band) is also part of the international (including Australia) unlicensed ISM bands [5]. Also, the 5 GHz transmission frequency, although free of the interference of the 2.4 GHz band, considerably limits its range (at the same power) compared to 2.4 GHz.

IEEE 802.11b

The second amendment, IEEE Std 802.11b - 1999, published in 2000, introduced specifications for higher data rates (5.5-11 Mbit/s) using direct sequence spread spectrum (DSSS) in the original 2.4 GHz international ISM band [5]. The 2.4 GHz band (2400–2500 MHz) is shared with Bluetooth devices, cordless telephones and other devices. However, unlike Bluetooth's 79 channels, IEEE 802.11b's DSSS spreads the data frame over a 22 MHz wide channel. Because of this wide DSSS signal, there are effectively only three non-overlapping channels that can be used in any given location and so it is highly prone to interference from other devices with similar spectra, including domestic microwave ovens.

IEEE 802.11g

While IEEE 802.11a is significantly faster than IEEE 802.11b, the two are incom- patible and IEEE 802.11b had, by far, the greatest market penetration [10, 11]. IEEE 802.11g [39] was a further addition, using IEEE 802.11a's Orthogonal Fre- quency Division Multiplexing over IEEE 802.11b's frequencies in the 2.4GHz ISM band. IEEE 802.11g can also fall back to IEEE 802.11b's DSSS operation and thus is fully backward compatible with IEEE 802.11b [3].

Super G

"Super G" is not an IEEE standard. Vendors, such as Others, Net- gear and D-Link use channel bonding, "which combines two 54 Mbps channels into one 108 Mbps [proprietary 'Super G'] link" [40]. "Super G" is thus incompatible with the standardized technologies, although such proprietary equipment will always offer the standard technologies as well. However, fall-back to the standard technologies may not necessarily be automatic.

V Other 802.11 Emerging Standards

This section briefly describes those amendments that were under development at the beginning of this research. Some of these have been completed and are described with the advances. Others are still ongoing.

IEEE 802.11e

Task Group E was developing Quality of Service (QoS) provisions for WLANs, which it completed in 2005, drawing on the additional management frames provided by Task Group H.

IEEE 802.11h

Task Group H was looking at the spectrum and power management for Europe, which it completed in 2003, providing new management frames also used by sub- sequent advances and directly related to this work.

IEEE 802.11i

Task Group I was working on the enhanced MAC security provisions, which it completed in 2004 and give the security to encrypted data during transmission.

IEEE 802.11j

Task Group J was adding regulatory requirements for use in Japan, which it completed in 2004.

IEEE 802.11k

Task Group K was investigating radio management information messages, which it completed in 2008, drawing on the additional management frames provided by Task Group H.

IEEE 802.11p

Task Group P is investigating "Wireless Access in the Vehicular Environment (WAVE)".

IEEE 802.11r

Task Group R was working on fast hand off between BSS APs to support streaming technologies such as VoFi. This completed in 2008, again drawing on the additional management frames provided by Task Group H, along with the radio management information messages from Task Group K.

IEEE 802.11s

Task Group S (TGs) is investigating wireless mesh protocols for access points, allowing for multi-hop transmissions via mesh routing protocols. Although the IEEE 802.11s standard is not ready yet, a number of vendors offer mesh networking products that allow enterprises to deploy WLAN APs in hard-to-cable locations or allow frequent movement of APs. Mesh

APs require power, but the only data cabling is on the edge of the mesh. Current solutions are unique to each vendor, whose hardware is not interoperable with others. Also, both back-haul and user access will contend for bandwidth, degrading performance.

IEEE 802.11v

Increasing uptake of WLAN will make management of enterprise-wide APs more difficult. There is a growing need for remote wireless network management of configurations and software. Typically, this is performed via the SNMP, but currently there are no standard MIBs for WLAN-specific parameters, so this varies from vendor to vendor. Currently, enterprises have to standardize on one vendor's hardware or else use a third-party tool that attempts to manage hardware from multiple vendors.

VI Proposed Work

The 4-way Handshake

The actual messages exchanged during the handshake are depicted in the figure and explained below

1. The AP sends a nonce-value to the STA (ANonce). The client now has all the attributes to construct the PTK.
2. The STA sends its own nonce-value (SNonce) to the AP together with a Message Integrity Code (MIC), including authentication, which is really a Message Authentication and Integrity Code (MAIC).
3. The AP constructs and sends the GTK and a sequence number together with another MIC. This sequence number will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
4. The STA sends a confirmation to the AP

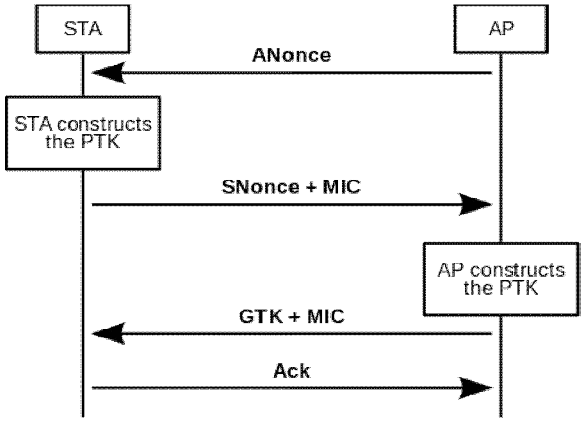

Fig 1 Handshake Process

The 4-Way Handshake is an essential component of the RSNA establishment. Its purpose is to confirm the possession of the shared PMK (Pair wise Master Key) in the authenticator and the supplicant, and derive a fresh PTK (Pair wise Transient Key) for subsequent data communication. In the handshake, the authenticator and the supplicant generate their own nonces and send them to each other. The PTK is derived from the shared PMK, the nonces, and the MAC address of the peers. Message 1 and 3 carry the nonce generated by the authenticator; Message 2 carries the nonce generated by the supplicant, and Message 4 is an acknowledgment to indicate the handshake is successfully completed. While Message 2, 3, and 4 are authenticated by the fresh PTK, Message 1 is unprotected. In order to prevent an adversary from affecting the PTK through forging Message 1, 802.11w adopts a Temporary PTK (TPTK) to store the newly generated PTK until Message 3 is verified. However, this approach does not prevent DoS attacks on Message 1. The supplicant must accept all Message 1 s it receives in order to ensure that the handshake can complete in case of packet loss and retransmission. This allows an adversary to cause PTK inconsistency between the supplicant and the authenticator by sending a forged Message 1 with a different nonce value between the legitimate Message 1 and Message 3. In order to accommodate the forged Message 1 s, the supplicant has to store all the responding nonces and the derived PTKs. Only after a Message 3 with a valid MIC is received, the supplicant can install the corresponding correct PTK for data communications and discard all others. Obviously, an adversary is able to launch a memory DoS attack by sending out numerous forged Message 1 s. This attack is serious because it is simple for the adversary to perform, and a successful attack will cancel all efforts in the previous authentication process.

The one-message attack on the 4-Way Handshake protocol

Message 1: AUTH ! SUPP
AA, ANonce, sn, "msg1"
Message 2: SUPP ! AUTH
SPA, SNonce, sn, "msg2", MICPTK(SNonce, sn, "msg2")
Message 1': Attacker ! SUPP
AA, ANonce', sn, "msg1"
[Supplicant generates SNonce', derives a new PTK' from SNonce' and ANonce']
Message 3: AUTH ! SUPP
AA, ANonce, sn+1, "msg3", MICPTK(ANonce, sn+1, "msg3")
[PTK and PTK' not consistent, MIC not verified, Protocol blocked]

Flow chart of 4-way handshake process

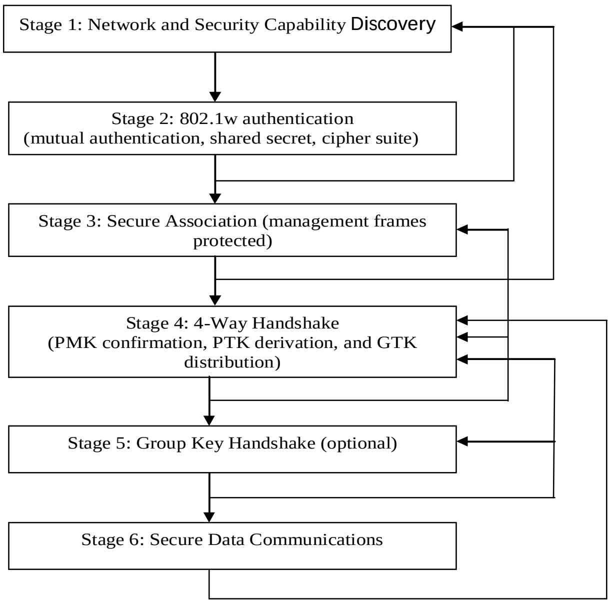
Stage 1: Network and Security Capability Discovery
Stage 2: 802.1w authentication
(mutual authentication, shared secret, cipher suite)
Stage 3: Secure Association (management frames protected)
Stage 4: 4-Way Handshake
(PMK confirmation, PTK derivation, and GTK distribution)
Stage 5: Group Key Handshake (optional)
Stage 6: Secure Data Communications

Fig 2 4-way handshake flow chart

RESULTS WAVEFORM

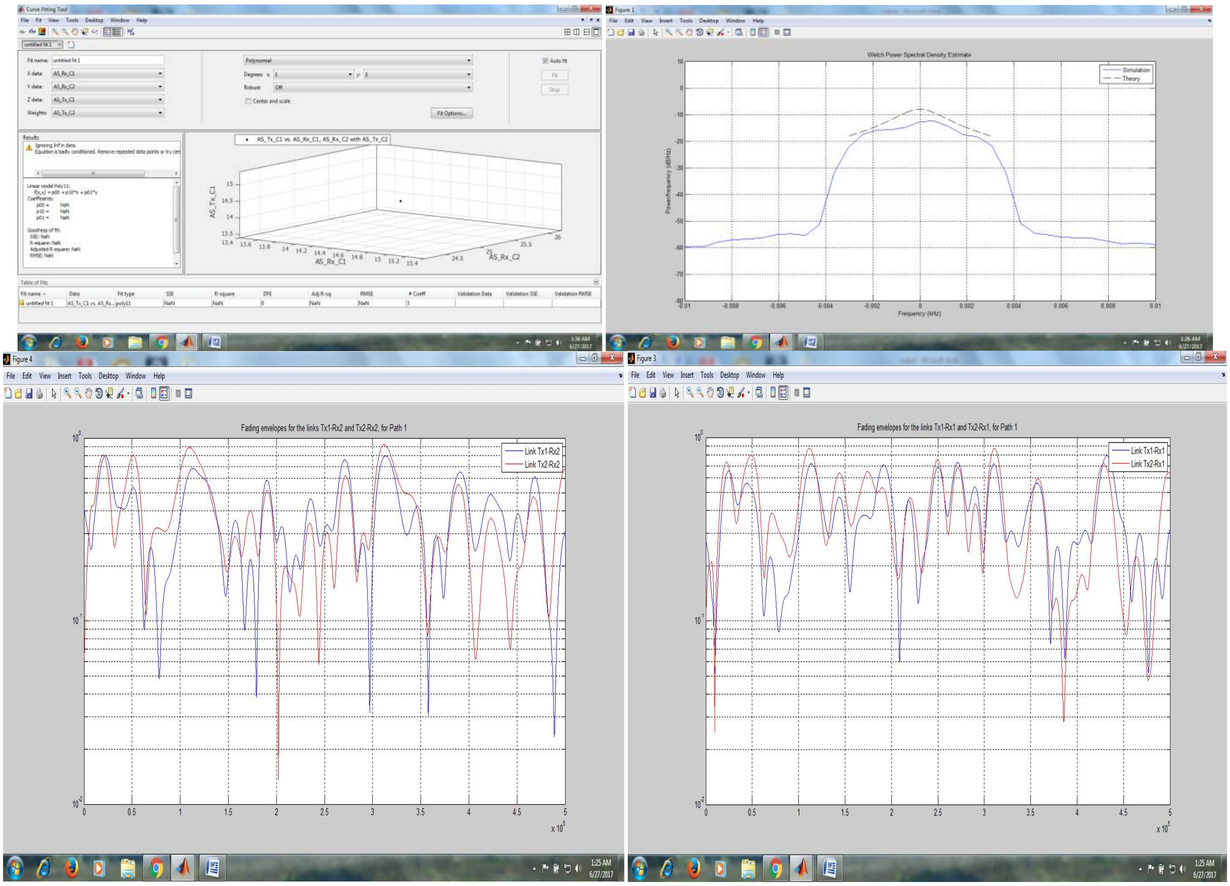
Curve Fitting Tool
AS_Tx_C1 vs. AS_Rx_C1, AS_Rx_C2 with AS_Tx_C2
AS_Tx_C1
AS_Rx_C1
AS_Rx_C2
Figure 1
Welch Power Spectral Density Estimate
Simulation
Theory
Power/frequency (dB/Hz)
Frequency (kHz)
Figure 4
Fading envelopes for the links Tx1-Rx2 and Tx2-Rx2, for Path 1
Link Tx1-Rx2
Link Tx2-Rx2
Figure 3
Fading envelopes for the links Tx1-Rx1 and Tx2-Rx1, for Path 1
Link Tx1-Rx1
Link Tx2-Rx1
x 10^5

Fig 3. Simulation Result

CONCLUSION

We described the procedure for finite-state verification of security protocols, and our results showed that this is a very effective approach. We identified the functionality of each field in the messages, in some cases supporting assertions made in the protocol documentation, and in a few cases suggesting alternatives. A simplified protocol was presented that has the same authentication properties as the original one under our Mure model. Most significantly, we found and analyzed an effective DoS attack on Message 1 in the protocol. As in many other case studies, this attack can be prevented by an extremely simple modification to the protocol. However, this clear improvement in the protocol was not apparent before our security analysis. The protocol is supposed to allow only one active handshake at any time and to generate a shared PTK between a corresponding supplicant and authenticator. However, upon analysis we showed that the supplicant must allow multiple handshakes to execute in parallel, in order to ensure protocol completion in the presence of packet loss. This leads to vulnerabilities, allowing an attacker to block the handshake by simply inserting one forged message. Furthermore, the attacker can construct a memory DoS attack if the supplicant is implemented to store the states of all incomplete handshakes. When 802.1 X authentications is implemented, the PMKID included in Message 1 will limit the attacker to constructing this attack only after the first Message 1 is seen in the link; Link Layer Data Encryption can protect the subsequent sessions after the first PTK is established. When both of these mechanisms are implemented, this attack can only be performed between Message 1 and Message 3 of the first legitimate 4-Way Handshake instance. These implementations cause more difficulties, but the attacker can still launch the attack if it keeps monitoring and intercepting the network in a timely way. However, since the attack can be prevented simply and completely, there is no need to live with a protocol subject to this attack.

References

1. Mathew, R., & Katkar, V., “Survey of low rate DoS attack detection mechanisms”. In Proceedings of the International Conference & Workshop on Emerging Trends in Technology (ICWET '11). ACM, New York, NY, USA, 955-958, 2011
2. Liu, J., Ye, X., Zhang, J., & Li, J., “Security Verification of 802.11i 4-way Handshake Protocol”, ICC 2008 proceedings, IEEE Conference, pp.-1642-1647, 2008.
3. Wang, L., & Srinivasan, B., “Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard”, Second International Conference on Networks Security, Wireless Communications and Trusted Computing, pp.-109-113, 2010.
4. Lashkari, A. H., Danesh, M. M. S., Samadi, B., “A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)”, 2nd IEEE International Conference on Computing & Processing (Hardware/Software), pp.-48 - 52, 2009.
5. Saini, H., & Panda, T.C., “Extended Cyber Defense Architecture for a University- A Case study”, The IUP

Journal of Science & Technology, Vol. 6, No. 2, pp. 33-47, June 2010.

6. IEEE Standard 802.11-1999. Information technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - Part 11: Wireless LAN Medium Access Control and Physical Layer Specifications, 1999.
7. IEEE Standard 802.11a-1999. Higher-speed Physical Layer in the 5 Ghz band, supplement to IEEE standard for information technology – Telecommunications and information exchange between systems - local and metropolitan area net-
8. Works - specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 1999.
9. IEEE Standard 802.11b-1999. Higher-speed Physical Layer extension in the 2.4 Ghz band, supplement to IEEE standard for information technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, September 1999.
10. IEEE Standard 802.11g-2003. Amendment 4: Further higher data rate extension in the 2.4 Ghz band, IEEE standard for information technology - Telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, 2003.
11. N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11. In the 7th Annual International Conference on Mobile Computing and Networking, July 2001.
12. L. Blunk, J. Vollbrecht, B. Aboba, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). Internet Draft draft-ietf-eap-rfc2284bis-06.txt, September 29 2003.

How to cite this article:

Sourabh patel and Hariom soni (2017) 'An Improved Mechanism For Four-Way Handshake Procedure In Ieee802.11w', *International Journal of Current Advanced Research*, 06(07), pp. 4640-4645.
DOI: http://dx.doi.org/10.24327/ijcar.2017.4645.0549

****