Research on Wi-Fi Security Protocols

Saurabh Malgaonkar
Computer Engineering Department,
Thadomal Shahani Engineering College,
Mumbai University,
Mumbai, India.

Rohan Patil
Associate Software Engineer,
Indus Valley Partners,
Mumbai, India.

Aishwarya Rai
Test Engineer
AMDOCS, Pune , India.

Aastha Singh
Associate Software Engineer,
Accenture, Bangalore, India.

ABSTRACT

Wireless local area networks (WLANs) with the gateway to internet services are becoming popular as they are fast, cost effective, flexible and easy to use. There are some challenges of security and for IT administrators the choice of security protocol is a critical issue. The main motive is to know about threats in the wireless security and be aware about the disadvantages of wireless security protocols. There is also a comparative analysis of WEP, WPA and WPA2. The check on the authentication of all 3 protocols by implying the legendary attack vector scripts i.e. Air crack set of tools is done. The test was conducted on Back Track operating system which is considered as dedicated pentesting operating system. In the test result, it was found out that WEP is the weakest, to which WPA was a temporary solution and WPA2 is a very solid and long term solution..

Keywords

Network security, security protocols, WEP, WPA, WPA2, WiFi Security

1. INTRODUCTION

In current network security research trends, the study of performance of security protocols of WLAN [1] has been one of research focuses. Whereas, owing to enormous complexity and low efficiency of modeling security protocols, there has been by now no uniform method or technology that can be used generally to simulate and evaluate security protocols. The protocols that are required to provide security to wireless networks can be implemented by creating a wireless scenario using the software Network Simulator. This paper illustrates a scenario to check the security protocol. As NS2 mainly has the implementation of routing protocols, a new protocol should be designed especially for security purpose. The security feature followed is encryption/decryption of the data that is being exchanged. Data should be ensured as and then there will be a perfect implementation of the protocol. So, the focus is on adding a new security protocol to NS2 and the implementation of that protocol by providing a wireless scenario. It also briefly describes the basic networks categories, analyzes the networks, briefly describes their components and technologies, explains the WiFi technology and analyzes property sources related to network simulator and its detailed description, specify the configuration for the simple network and create corresponding model by using NS2 simulator, demonstrates selected characteristics of the specified network configuration using the simulation model, and show scenario of transmission data among nodes. The language used in this paper to simulate tool. Finally to show facility of simulate uses cryptography to secure information packets transfer among nodes using C++ language to process because faster than tc. In today's situation, all tasks which were usually carried out offline have been shifted to online. This paradigm shift [2] has lead to personal details such as bank account, email, online money stored by individual organizations for transaction purposes. The need for security on any network is apparent. The prevention of insecure network and the desire for confidentiality, integrity and availability is the main focus. However, the problem that already exists are added too, when one adds wireless network. As wireless networking becomes more popular, the flawed security [4] of most of those network becomes apparent. The overall aim is to study and understand the currently existing standards for wireless communication. Various parameters and scenarios over which the performance of a protocol can be evaluated are selected. Through the results obtained from this process it is easy to identify whether the performance and security measure of the improved protocol is better than the currently operational ones. In this paper NS2 tool is used as a method to virtually create a network wherein the protocols can be simulated and test results can be reported. NS2 provides results in 2 formats, namely 'nam' and 'X-graph'. Nam will execute the protocol implemented over the nodes and show animations of the file transfer between the nodes in the closed network. X-graph however will give the performance analysis on the parameters which we have set. Also in this paper there is a detailed explanation of WEP, WPA and WPA2 security algorithms. These algorithms forms the foundation for the security protocol design. Hence it is important to understand every aspect of the algorithm in order to further make changes and help the particular protocol become more efficient.

2. SECURITY METHODS REVIEW

2.1 WEP

WEP protocol [5] is the basic part of IEEE 802.11 (IEEE – Institute of Electrical and Electronics Engineers) standard for the protection of WLAN networks. The basic function of WEP protocol is to provide data security in wireless networks in the same way as it is in the wired networks. Lack of physical connection among users and wireless networks enables all users within the network range to receive data if they have appropriate receivers. The only possible way to protect this kind of network was to create a protocol that would work on the second layer of OSI model and, in this way, provide the data protection during the transmission. In order to protect data transmitted among the communicating parties, WEP uses shared secret key of 40 to 140 bits. WEP protocol is applied through the following three steps :

- CRC (Cyclic Redundancy Code) message is calculated and added to the original message.
- The second step in WEP protocol application is encryption (as shown in Figure 1). The message is encrypted by RC4 algorithm. Encryption is d one in three phases. First, pseudo-random data sequence of three bytes is generated (IV – Initialization Vector) to extend the key. Encryption ends with the application of exclusive or function (XOR) between keystream and message thus resulting in encrypted message.
- The last step is to transmit sequence IV and encrypted message. Once the message has come to its its final destination, the reverse procedure is applied. Again, the extended key is generated on the basis of transferred IV and shared key; then RC4 algorithm generates keystream, XOR function is calculated between keystream and message that arrived.

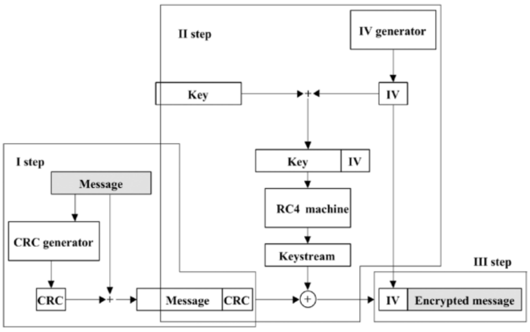

Fig 1: WEP protocol execution

Open System Authentication enables mobile stations to access the access point without confirmation of the station’s identity. This is a one-way authentication since mobile stations believe to communicate with the right access point. Open System Authentication is very sensitive to attacks and allows unauthorized access. Shared-key Authentication is based on encryption technique and on questions and answers procedure between a station and the access point. The authentication process is ended when the access point decrypts the station’s answer by shared key and thus enables the access of the workstation only if decryption result is equal to the question that has been sent In 802.11 standards the confidentiality is realized by encryption technique. WEP protocol for the protection of confidentiality uses RC4 algorithm and symmetrical key together with pseudo sequence. In general, every increase in key length brings the increase in protection. However, recent brute-force attacks on wireless local networks are jeopardizing privacy. This means that WEP protocol is sensitive to attacks no matter of the key length. WEP protocol provides integrity of messages transmitted between stations and access point by using CRC technique. Integrity of message received is violated when the checksum differentiates. In this case, the message received is rejected.

2.2 WPA

IEEE studied all details of WEP security problems and focused on the design of new safety mechanisms for wireless networks. The solutions are offered in 802.11i standard. However, standard issuance and rectification can take a few years and the market makes a pressure on manufacturers so that they are not in a position to wait for standard issuance and ratification to be finished. In order to solve this problem, Wi-Fi defines WPA [6] (Wi-Fi Protected Access) standard to improve the protection of wireless devices. WPA has contributed to the increased protection of wireless communications through the increased level of data protection and access control of current and future solutions to wireless networks. WPA is designed to be the software upgrade to the existing devices and is compatible with the new IEEE 802.11i standard. WPA has several purposes:

- To be a strong protective mechanism for wireless networks,
- To be interoperable,
- To replace WEP,
- To enable the existing Wi-Fi wireless devices to be upgraded with the new software solution,
- To be applicable in small, as well as in large wireless networks, and
- To be applicable immediately.

The first improvement offered by WPA is data encryption by TKIP (Temporal Key Integrity Protocol). This protocol provides a strong encryption mechanism whose characteristics are:

- A unique stream for encryption of each of the packets,
- Message integrity check (MIC, Michael),
- IV extension, and
- Repeated key mechanism.

The second improvement is related to the strong security authentication of the users through 802.1x and EAP(Extensible Authentication Protocol). In large networks, WPA uses authentication server RADIUS to secure centralized management and control of the access. In small SOHO (Small Office/Home Office) networks, there is no centralized authentication server so that WPA is initiated by a special mode. This mode is also called Pre-Shared Key (PSK) and it enables users to authenticate by a password or a key. Users have to enter a password (or a key) to the access point, otherwise home network reaches each of the workstations included in the Wi-Fi wireless network. Devices with appropriate password can be networked and thus protected from eavesdropping and other unauthorized users.

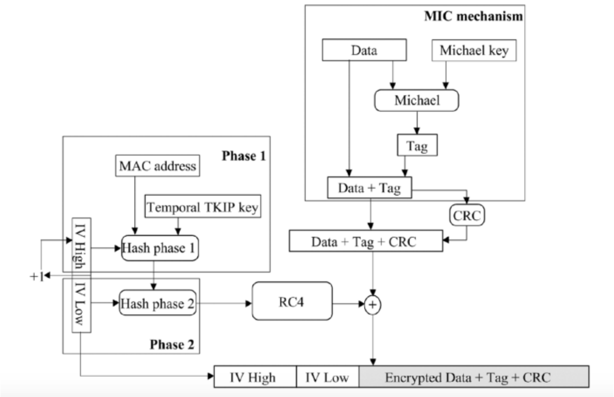

Fig 2: WPA protocol (WEP safety improvements)

2.3 TKIP

TKIP [7] is a collection of algorithms created to improve and solve security problems of WEP. Majority of cryptographic functions is realized through hardware in wireless networks adapters, thus it is not possible to improve the hardware.

RC4 is an encryption device implemented in hardware of wireless network adapters and is not replaceable. To solve this problem TKIP uses RC4 device in the way that changes the methods of use of the shared key. In WEP, shared key is used directly in encryption, while in TKIP it is used for generation of other keys. TKIP algorithms can be applied in the current wireless equipment without significantly ruining the performance. TKIP gives WEP four new improvements :

- Encrypted message integrity code to prevent message falsifications,
- Strict IV sequences to prevent replay attacks,
- Key generation, and
- Mechanism to refresh keys in order to prevent
- attacks related to key repetition. Encrypted message integrity code (MIC). MIC is an encryption mechanism based on hash function design to work on existing wireless network adapters in order to detect false messages. MIC mechanism consists of three components:
- authentication key (Michael key, both the
- sender and the receiver have the same key),
- tag function, and
- verification.

Tag function generates the tag based on the authentication key and message. Generated tag is an encryption for integrity check and is sent together with a message. Receiver performs MCI strength is in the number of tag bits (n). This means that if the attacker wants to send a false message, 2n messages have to be sent . MIC has a level of protection of n = 20, while the strongest attacks could generate 229 messages. It is obvious that MIC with the above given level of protection is not completely safe. Therefore, TKIP implements mechanisms for detection of false messages and in case there are two false messages in a second, it is considered to be an attack. In that situation keys must be erased, session must be terminated and one minute has to pass before the new session with the new TKIP and Michael keys is established. Strict IV sequences. False messages appear when the attacker meets the message and sends it as his own. Usually, this problem is solved by linking IV counter with the MIC key. Each time the MIC key is replaced, IV sequence is reinitialized. This strategy requires the transmitter to stop its transmission when the same IV sequence repeats for one MIC key. This happens when communications ceases or MIC key changes. TKIP affects IV sequence. Transmitter and receiver set IV to zero each time TKIP key is changed. Sender increments IV sequence for each packet that is sent. TKIP requires receiver to supervise all sequences of the IV sequence that has just arrived. If the newly arrived IV sequence is smaller or even the same as the previous IV sequence for the same TKIP key, or if IV sequences arrive in no logical order, then it is a reason to dismiss these messages. In WEP protocol a unique key for each packet is based on concatenation of unchanged key and IV sequence. As a result of this key generation there is his often repetition. For each of the packets a new key is generated by hash function based on TKIP key and IV sequence. It is called temporal key since its duration is temporal and it changes when its time elapses. Key generation in TKIP protocol has two phases

- In phase 1, hash function is calculated based on the MAC address of the sender, temporal

session key and high 32 bits of IV. This phase is calculated only if temporal key of the session is changed.

- In phase 2, hash function is calculated by the phase 1 output and low 16 bits of IV. As an output, we have a key stream of 128 bits. In fact, the first 3 bits of phase 2 are compatible with IV in WEP, while the remaining 13 bits are compatible with WEP. The purpose of phase 2 is to make it difficult for the attacker to find correlation between IV and a key for each of the packets. The analysis of C code that implements both phases shows that some of the cryptographic characteristics of S-box have been applied .

TKIP mechanism has three keys:

- Temporal key,
- Encryption key
- Master key.

Temporal keys are 128 bit encryption key and 64 bit key for encryption of data integrity. TKIP uses separate key sets on both sides of connection, so that there are four temporal keys in total. TKIP identifies these sets of keys by 2 bit identification device named WEP keyid. When first connection is established, the first set of keys is immediately connected to one of the two sets of WEP keyid. When a new set of keys is created, a new keyid is distributed to it. After the connection between a new pair of temporal keys is established TKIP implementation will continue to receive packets on the old keyid and its keys. However, later on, the transfer will be conducted only via new keyid and its keys. New temporal keys are created with the first or repeated establishment of connection. Encryption key protects temporal keys. There are two of these keys – one is used to encrypt the message to introduce temporal keys, while the other serves to protect the message from being falsified. Master key is exchanged among workstations and 802.1x authentication servers. This key is directly related to authentication and is used for secure distribution of key streams. Master key is created after a successful authentication and is related to one session only.

2.4 802.1x

IEEE 802.1x [8] is standardized way to the network secure access. By using security methods in 802.1x standard it is possible to access the network securely, even when products of different manufacturers are in use. 802.1x is only a part of security technology that disables unauthorized access to the network and does not control traffic of the authorized users. 802.1x does not require a specific authentication protocol, but uses EAP for encapsulation of other authentication protocols (LEAP – Lightweight Authentication Extension Protocol; EAP-TSL – Transport Layer Security; EAP-TTLS – Tunneled TLS; EAP-PEAP – Protected EAP). A successful authentication , both of a client and authenticator, has to be completed before any traffic from the client is allowed. Before authentication 802.1x logical component (PAE – Port Access Entry) prohibits any traffic except for the EAP request that is being forwarded to the authentication server. Based on the EAP message, authentication server determines whether a client has or does not have an access to the network. Then it sends a message to the authenticator and, based on the message, the port is either in the position to prohibit or approve the traffic. Previously researches have showed that primary Authentication method (open authentication system and shared key authentication) and access control based on MAC control lists are not secure mechanisms. In order to solve the problem, IEEE group designed new security architecture for wireless local networks – Robust Security Network (RSN). RSN provides a mechanism for connecting to the network only through an authorized 802.1x network port. Network port represents a connection between the station and AP. RSN uses three entities define by 802.1x standard: station, authenticator and authentication server. The station is an entity that wants to access the network through authenticator's network port (access point). The station is authenticated through authenticator on authentication server from which it receives accreditations.

RSN connection is performed in three phases:

Phase 1: Request, authentication and association. The station looks for the AP with appropriate SSID. All APs in the range answer with the Probe Request framework.

When the station identifies with which AP it is connected and accepts its parameters, authentication is performed as well as connection to the AP. At the end of phase 1 the workstation and the AP establish security rules and 802.1x authentication port is locked. 802.1x network port remains locked as long as the authentication procedure has been completed.

Phase 2: 802.1x authentication. In this phase the station is authenticated with the authentication server. The station and the AP have to authenticate mutually in order for the station to escape false access points and for the access points to escape false stations. 802.1x standard uses EAP for different authentication mechanisms. In communications between the station and the authenticator, EAP protocol uses four messages: EAP Request, EAP Response, EAP Success and EAP Failure. EAP can route messages to the authentication server (such as RADIUS) through 802.1x port when it is locked. EAP packets between the station and the authenticator encapsulated EAPOL (EAP over LAN) packets, while EAP messages between authenticator and authentication server are encapsulated in RADIUS packets. The station sends EAPOL start message to the authenticator. Based on this message, the authenticator requires station identification. The station then replies with identity parameters that are forwarded to the authentication server by authenticator. Then the mutual authentication between the station and authentication server is done. If the mutual authentication is successful, the authentication server generates Master Session key (MSK) and forwards it to the authenticator and to the station. PMK (Pair-Wise Master Key) is then generated by the station and authenticator based on the MSK. Phase 3: 4-Way Handshake. The station and the authenticator have to mutually confirm the current PMK in order to complete successfully RSNA . After successful confirmation a PTK (Pair – Wise Transient Key) is generated to be used for a secure transfer of session data. Now 802.1x port is unlocked. 802.1x authentication has several advantages:

- Administrators can define users' responsibilities in the network, they do not have to pair manually users' names with MAC addresses,and can easily find mistakes and supervise the network.
- Administrators allow access to the network according to the manufacturer standards.
- An authorized port cannot be compromised by a non-802.1x client.
- The authenticator waits for a certain period of time for a client to re-authenticate before the port is locked.
- A continuity of authentication procedure is allowed in case the client was temporarily unable to respond to authenticator's request.
- It is allowed for more devices to access the network by a shared mediator (such as hub), and
- Protection is imposed to all users of the access point.
- In addition to the advantages mentioned before, 802.1x authentication has also some deficiencies. These deficiencies result from the mistakes in 802.1x and EAP protocols that the attackers have used for attacks.

3. EXPERIMENTAL DESIGN

Using the network simulator NS2 [9], the attacks in the WSN can be simulated. NS2 creates a replica of a real time network. It is a time based event driven simulator. The code can be written in such a way that at what time, what particular event can happen. The nodes can be created, the data transfer between the nodes and the attacks can be shown. It has become one of the most widely used open source simulators. It is a free simulation tool that can be available online . The simulator consists of a wide variety of applications, protocols like TCP, UDP and many network parameters. It runs on various platforms like UNIX, Mac and windows platforms. This NS2 tool allows to develop a model design for wireless sensor network connection between nodes in the network. Based on the network attacks like denial of service, flood attack, sinkhole attacks, Sybil attack the network security can be tested. These attacks can be created in the network and the security level of the wireless sensor network can be tested to ensure secure data transmission between the nodes in the network. The WEP, WAP and WAP2 security protocols are the primary focus areas. The advantages and limitations of the same are an important feature in this project. Security of any system depends on the encryption method used by that protocol. NS2 is a network simulation tool which helps to analyze and design network configurations. Design of wireless Network uses NS2, as a base on Security evaluation, and describes the proposed model of the system and complete description of the Simulations and software program needed for implementing the Network. Ns-2 is a widely used tool to simulate of networks. Network simulator is a part of software that predicates the performance of a network without a real network being there. NS2 is a vital simulation tool for networks. It supports a number of algorithms for routing and queuing. NS2 is very helpful because it is very costly to verify viability of new algorithms, test architectures, check topologies, check data transmission etc. Network simulators are names for series of discrete event network simulators and are heavily used in ad-hoc networking and support popular network protocols, offering simulation results for wireless networks. Also using security in the network the basic conceptions in the security of the network, then it discusses encryption and decryption concept the implementation of non-conventional (both blocks and stream ciphers) The reason for having two programming languages from the aim is to have an easy to use, yet fast and powerful simulator. C++ forms an efficient class hierarchy core of ns-2 that takes care of handling packets, headers and algorithms. Object Tcl, or OTcl, is also an object oriented programming language utilized in ns-2 for network scenario creation, allowing fast modifications to scenario scripts. OTcl and C++ interact with each other through Tcl/C++interface called Tcl/C++

3.1 Method Implementation

For the implementation of WEP and WAP2 we have to discuss and understand 2 algorithms which form the core in operations of respective protocols. It is important to understand these two methods before we go further and implement them on NS2.

RC4 method of encryption-

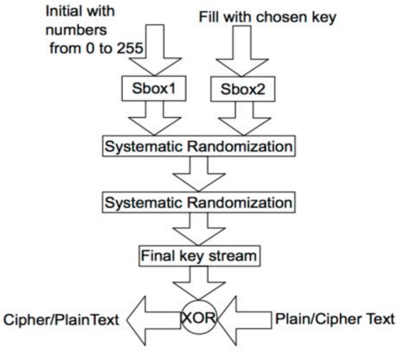

Fig 4: RC4 Flowchart

is encrypted. The initialization process can be summarized by the pseudo-code

```
k = 0;
for s = 0 to 255:
d[s] = s;
for s = 0 to 255:
k = (k + e[s] + d[s]) mod 256; swap d[s] and d[k];
```

It is important to notice here the swapping of the locations of the numbers 0 to 255 (each of which occurs only once) in the state table. The values of the state table are provided. Once the initialization process is completed, the operation process may be summarized as shown by the pseudo code below;

```
s = k = 0;
for (v = 0 to N-1) {
s = (s + 1) mod 256;
k = (k + d[s]) mod 256;
swap d[s] and d[k];
pr = d[ (d[s] + d[k]) mod 256]
output M[v] XOR pr
}
```

Where M[0..N-1] is the input message consisting of N bits.

This algorithm produces a stream of pseudo-random values. The input stream is XORed with these values, bit by bit. The encryption and decryption process is the same as the data stream is simply XORed with the generated key sequence. If it is fed in an encrypted message, it will produce the decrypted message output, and if it is fed in plaintext message, it will produce the encrypted version . This algorithm produces a stream of pseudo-random values. The input stream is XORed with these values, bit by bit. The encryption and decryption process is the same as the data stream is simply XORed with the generated key sequence. If it is fed in an encrypted message, it will produce the decrypted message output, and if it is fed in plaintext message, it will produce the encrypted version . TKIP method of encryption-

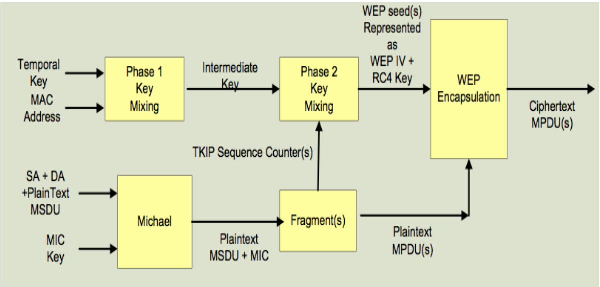

Fig 5: TKIP Flowchart

A) Message Integrity Code-

Defeat Forgeries

1. Secret Key(m1 an m2)
2. Tagging function-pads message to multiple of 32 bit
3. Verification-counter measure checks for forgery.

B) IV sequence-

1. Packet sequence number
2. If packet sequence number is less than or equal to previous MPDU associated with key =>> set replay unit

C) Per packet key mixing-

1. A combination of MAC address and Temporal address will result in creating an Intermediate key

Encrypts packet sequence number and generates 128 bit per packet key

3.2 Result Analysis

To practically understand how WEP and WPA perform in real world situations following operations have been carried out with 20, 30, 50 nodes (computers in operation). All the factors remain same both the protocols are implemented and evaluated. X-graph of NS2 is utilized for evaluating the throughput for the WEP protocol hence implemented. This section deals with results obtained when the security algorithm is WEP employing different number of nodes. The results so obtained are plotted using X-graph utility in NS2. The results show the variation in throughput when 10 number of nodes have been considered for the wireless LAN. As inferred from the plot , the throughput initiates 10 second after commencement of the simulation. After initial connection set-up phase, the nodes start moving in different directions due to which the throughput initially drops down then rises steadily with a small slope. Reasonable throughput levels have been achieved at simulation time of 20 seconds with peak performance lying between 40 to 50 seconds. The average throughput during the complete simulation is found to be 419.02 Kbps.

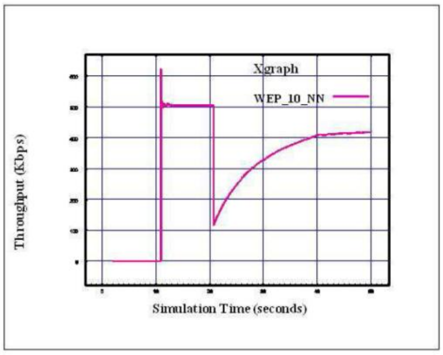

Fig 6: WEP = 10 nodes

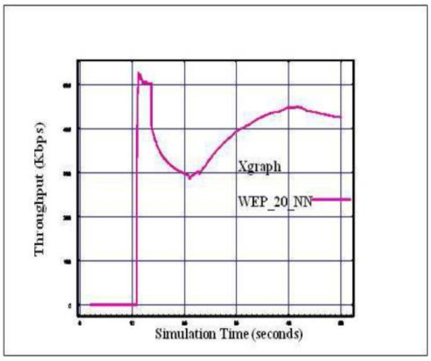

Fig 7: WEP = 20 nodes

Similarly when numbers of nodes in wireless LAN are considered to be 20, the variation can be plotted as shown. In this case, the average throughput during the complete simulation comes out to be 425.01Kbps Finally, a SOHO network comprising of 30 nodes is considered using WEP as a security algorithm. Total simulation time taken is 50 seconds and all nodes are wirelessly connected to each other. The variation is plotted as given where it is noticed that the throughput increases steadily after 25 seconds of simulation time and the average value for this simulation is computed as 425.06 Kbps. The results have been computed for WPA security algorithm, employing different number of nodes.

The results obtained are plotted using X-graph utility in NS2. The results show the variation in throughput when the scenario comprises of 10 numbers of nodes. The documented results illustrate similar variation as has been computed in case of a wireless LAN set-up comprising 10 nodes while employing WEP as the security algorithm with a differentiation that there is a decrease in throughput. The average value of the throughput in this case has been computed as 339.23 Kbps. Similarly when numbers of nodes have been considered of double the value, i.e., 20, the variation with respect to throughput being computed has been depicted.

The variation in throughput for WPA is similar as that of WEP but again a dip is seen in the throughput, with an average throughput of 407.8 Kbps. Finally, a SOHO network is considered comprising 30 nodes while using security algorithm as WPA. Here total simulation time is 50 seconds when all the nodes are assumed to be wirelessly connected to each other and the variation has been plotted as shown.

In this case too, a similar observations have been are observed; firstly variation in throughput for WEP and WPA are similar and then a dip is observed for WPA protocol. The average throughput for this set-up is found to be 359.8 Kbps

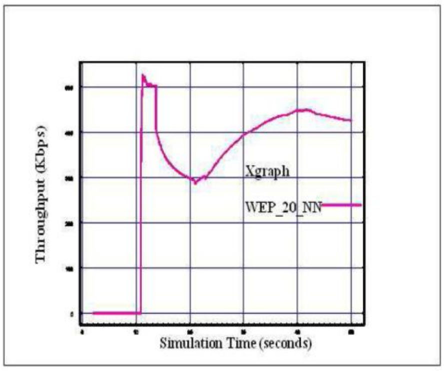

Fig 8: WEP range = 30 nodes

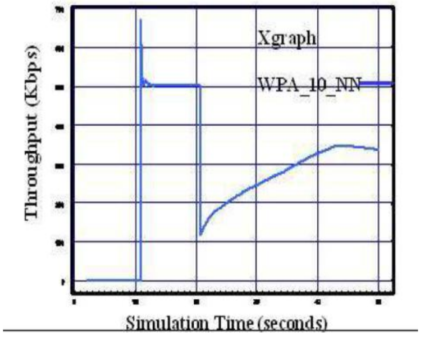

Fig 9: WPA range = 10 nodes

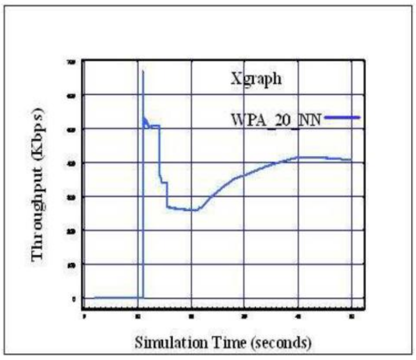

Fig 10: WPA range = 20 nodes

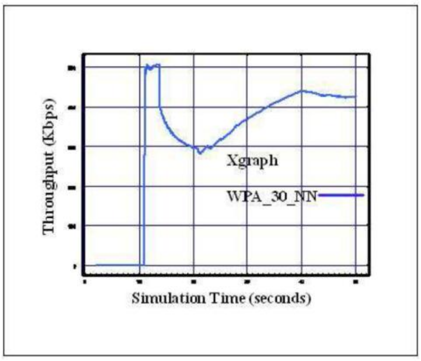

Fig 11: WPA range = 30 nodes

4. CONCLUSION & FUTURE WORK

A combination of different scenarios and situations to evaluate the standards of current protocols. There is a virtual creation of a network of nodes with SOHO networks in different ranges. For three variety of ranges and sizes of nodes first performance of WEP is benchmarked. The readings are done through X-graphs. For the second phase of this research WPA-2 is to be tested keeping the whole environment identical. The results thus obtained will be evaluated by using a bar graph. Extension of this work:

1)To evaluate the WPA-2 against specific and more vivid parameters to exactly understand its limitations.

2)By reporting the situation wherein it under performs certain modifications can be made to improve its performance in that scenario. However it is also important not to affect this change in areas where it is working correctly. After each iteration it is necessary to perform the above mentioned operation so as to uncover new results and its affect on the transmission and security of the data item.

3)The process that is followed will be standardized to evaluate new modifications made by any individual organizations to check the performance of their network. Establishment of such a process scheme will allow independent organization carry out research and declare results thus improving WPA for everyone to use.

5. REFERENCES

[1] J. WELCH , S. D. LATHROP , A Survey of 802.11a Wireless Security Threats and Security Mechanisms. United States Military Academy West Point , New York, (2003), http://www.itoc.usma.edu/Documents/ ITOC TR-2003-101 (G6).pdf.

[2]J. C. CHEN , M. C. JIANG , Y. W. LIU , Wireless LAN security and IEEE 802.11i. IEEE Wireless Communications , (2005) , vol. 12, no. 1, pp. 27–36.

[3] R. PRODANOVIC , D. SIMIC , Holistic Approach to WEP Protocol in Securing Wireless Network Infrastructure. Com SIS , Vol. 3, No. 2, pp. 97–113, (2006)

[4]C. HE , J. C. MITCHELL , Security Analysis and Improvements for IEEE 802.11i. Stanford, USA, (2004), http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/NDSS05-1107.pdf

[5] WEP Fix using RC4 Fast Packet Keying. RSA Laboratories,(2002), http://www.comms.scitech.susx.ac.uk/fft/crypto/wep.pdf

[6] White paper: Testing for Wi-Fi Protected Access (WPA) inWLAN Access Points. Net-O2 Technologies, (2004), http://whitepapers.zdnet.co.uk/0,39025942,60152756p,00.html

[7] W. HAN , D. ZHENG , K. CHEN , Some Remarks on the TKIP Key Mixing Function of IEEE 802.11i. Cryptology ePrint Archive , (2006), http://eprint.iacr.org/2006/129.pdf

[8] M. ARUNESH , A. W. ARBAUGH , An Initial Analysis of the IEEE 802.1X Standard. Maryland, (2002),http://www.cs.umd.edu/~waa/1x.pdf

[9]"Network Simulator 2", http://www.linuxjournal.com/article/5929,December 2015.

6. AUTHOR PROFILE

Saurabh Malgaonkar is an assistant professor in the computer engineering department of the Thadomal Shahani Engineering college which is affiliated to the Mumbai University. His areas of interest are: Networks and Distributed Computing.

Rohan Patil is a software developer in Indus Valley, a IT company, his areas of interest are networking and software development.

Aishwarya Rai is a software testing engineer in AMDOCS, her areas of interest are software development and testing.

Aastha Singh is an associate engineer in Accenture, her areas of interest are Cloud Computing (SalesForce).