Impact of New Highly Secure Scheme on Wireless Network 802.11 Performance

Brijesh Singh Yadav
UPRVUNL
Lucknow, U.P. (India)

Parul Yadav
Amity University,
Lucknow, U.P. (India)

ABSTRACT
Wireless local area networks (WLAN) are beginning to play a much larger role in corporate network environments and are already very popular for home networking applications. This increase in accessibility has created large security holes for hackers and thieves to abuse, that is finally being addressed by stronger security protocols and these security protocols include Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and 802.11i (WPA2). In this paper, we investigate the performance of wireless local area networks (WLANs) and security protocols available for WLANs. These existing security protocols have certain vulnerabilities and often hamper network performance as maintain poor trade-off between security and overhead on network performance. Here we propose our security protocol Slot Based Security Scheme (SBSS) in wireless local area network. Our proposed security protocol SBSS drastically increases the security and incurs almost same overhead on network performance as other existing security protocols in WLANs. We also develop our simulator in c++ to examine the impacts of these existing security protocols and our proposed protocol SBSS in WLANs on network performance that proves that our proposed scheme SBSS is much more efficient than existing security protocols in WLANs as SBSS maintains good trade-off between security and its associated overhead incurred on network performance.

Keywords
Wireless Network Security, Encryption Overhead, RC4, AES, TKIP

1. INTRODUCTION
With wireless LANs, users can access shared information without looking for a place to plug-in. Wireless LAN offers productivity and convenience like mobility, installation speed and simplicity, installation flexibility, reduced cost of ownership, scalability over wired networks [11,12]. Wireless networks have exhibited significant growth within the last few years in both home and corporate environments due in part to low cost and increased hardware quality. This growth has fueled new applications for wireless networks ranging from advanced warehouse inventory systems to wireless voice over internet protocol (VoIP) phones. The ease of use and vast distribution of these systems has created a security nightmare for home users and network administrators, which has become widely publicized in the media. With increase the popularity of wireless network the desired security level also increasing so this paper is exploring three popular standards for security in wireless local area networks that include Wired Equivalent Privacy (WEP) [3], Wi-Fi Protected Access (WPA) [1, 3], WPA2 [6, 7, 9] with its advantages and disadvantages. To counter the vulnerabilities in existing security protocols in WLAN and to maintain trade-off between security and overhead on network performance, in this paper, we propose and discuss a new security protocol in wireless local area network. Here, we also compare this new security protocol to exiting security protocols in wireless local area network.

This paper is organized as follows. Section 2 points out strengths and weakness of existing security protocols in wireless local networks. In section 3, we describe and analyze in detail our proposed security protocol in wireless local area network. Section 4 summarizes the simulation details that are utilized for the performance measurement and evaluation of our security protocol. In section 5, our simulation results show that the drastic increase in security using our proposed protocol SBSS incurs almost same overhead as existing most secure protocol in WLAN. Section 6 presents a discussion of the results from previous and concludes that our objective to maintain trade-off between security and associated overhead due to SBSS on network performance efficiently fulfilled. This section also recommends areas for future work.

2. WIRELESS SECURITY STANDARDS

2.1 Wireless Equivalent Privacy (WEP)
WEP is an encryption algorithm developed by an IEEE volunteer group. The aim of WEP algorithm is to provide a secure communication over radio signals between two each end users of a WLAN. WEP uses two key sizes: 40 bit and 104 bit; to is added a 24-bit initialization vector (IV) that is transmitted directly. WEP is a protocol that utilizes RC4 encryption and a 24 bit IV. It began with a 40 bit key that was later expanded to 104 bits. The keys it uses are called Preshared Keys (PSK). The keys are manually entered. WEP adds a checksum of 32 bits called the Integrity Check Value (ICV) to the end of a packet. The authentication method is weak and even helps attackers decipher the key [3]. Another problem with WEP is that we have to manually configure the key for each wireless device used. This can be problematic if a key is compromised in a large network relying on that key because every device on the network must have their keys changed that creates a logistical in a university or enterprise setting. This discourages organizations from implementing WEP. It also discourages organizations using WEP from ever changing keys.

After some years of the implementation of WEP, many flaws like insecure ICV, IV key reuses attack, known plaintext attack, partial known plaintext attack, authentication forging, dictionary attacks, real-time decryption etc. [12] were discovered in it. In next subsection, we discuss the Wi-Fi Protected Access (WPA)[6,5] that have advantages over WEP.

2.2 Wi-Fi Protected Access (WPA)
WPA was created by the Wi-Fi Alliance once the flaws associated with WEP were discovered, and used as an intermediate standard until the IEEE 802.11 working group developed a more secure protocol. WPA was based on the WEP protocol, but utilizes the stronger encryption technology used in TKIP [7], that offers pre-packet key mixing and a message integrity check. WPA works to address the

shortcomings of WEP. WPA supports authentication through 802.1X [2] (known as WPA Enterprise) or with a preshared key (known as WPA Personal), a new encryption algorithm known as the Temporal Key Integrity Protocol (TKIP) [7], and a new integrity algorithm known as Michael. WPA is a subset of the 802.11i specification. TKIP takes the original master key only as a starting point and derives its encryption keys mathematically from this master key. TKIP then regularly changes and rotates the encryption keys so that the same encryption key is never used twice. This all happens in the background automatically, invisible to the user.

Many flaws like birthday attack, differential cryptanalytic attack, lost RC4 keys problem [15], DOS attack etc are faced in WPA. Some encryption flaws in WPA due to RC4 encryption method are removed by using WPA2 that is discussed in next subsection.

2.3 802.11i (WPA2)

This is essentially the certified name for IEEE 802.11i by the Wi-Fi Alliance, and can be thought of as synonymous with IEEE 802.11i [6,7]. The main difference between WPA and WPA2 is the requirement of CCMP encryption with WPA2. Like WPA, WPA2 is also available in Personal and Enterprise modes. WPA2 allows an easy transition from WPA mode by using WPA/WPA2 mixed mode, so networked computers can use either WPA or WPA2. It doesn't employ RC4 like WEP or WPA; it uses Counter Mode with CBC-MAC Protocol (CCMP) to encrypt network traffic. CCMP employs Advanced Encryption Standard (AES) as encryption algorithm [9,16]. 802.11i is backwards compatible with WPA but not with WEP. Thus WPA2 is most secure among existing security protocols but has few complexities related to its encryption overheads. High power consumption is still posing problems in WPA2. The overhead associated with WPA2 is increased drastically due to this strong AES mechanism in this protocol. Like WEP, WPA2 also uses only one algorithm and one key to encrypt and decrypt the all the packets. Thus if the mechanism is compromised once, it can not be maintained back. Thus it is also not maintainable. Moreover, when the network is large that is we are having large number of nodes in the network, overhead on network performance associated due to WPA2 will be very high. In order to maintain trade-off between security and overhead on network performance and to overcome certain vulnerabilities in existing security mechanisms in wireless local area network and, we propose our new Slot Based Security Scheme that provides very high security in comparison to WPA2. Moreover, as network size grows, overhead associated due to SBSS downs to decrease rapidly in comparison to WPA2.

3. PROPOSED MECHINISM

In this section, we describe our new proposed security mechanism in wireless local area network. This proposed security mechanism is named as Slot Based Security Scheme (SBSS). SBSS uses four Encryption/Decryption algorithms namely, RC4, RSA, Blowfish and AES; and randomly selects one of these four algorithms at a time for encryption/decryption. Unique 2-bits code is assigned to each algorithm. Instead of actual names of the algorithms, this 2-bits code discriminates among these four algorithms. We use 256 slots. Each slot randomly stores one of four 2-bits codes as shown in figure 1.

01	00	……		11
Slot0				Slot 255

Figure 1. Slot structures of SBSS

00: RC4, 01: AES, 10: RSA, 11: Blowfish

In SBSS, we also store four different key-lists one for each of these four algorithms. Each message is encrypted with a randomly selected algorithm and a randomly selected key. Number of slots is taken 256 just to maintain trade-off between security and its associated overhead. Thus any hacker needs to go through the interception of a larger number of 4^{256} possible combinations just to figure out the exact formation of the slots even before he starts to consider any key attacks (like brute force attack).

3.1 Header Structure

SBSS header consists of three parts as shown in figure 2. The first part is the key selector (KS), second part is slot sector (SS) and the third part is data payload. The first part is 48-bit long to select among 2^{48} keys. The second part, that is 8 bit long, contains address of the selected slot among 256 slots of the slot structure. This selected slot contains the code for algorithm that will be used for encryption and decryption.

KS	SS	Data payload

Figure 2. Header Structures of SBSS

In next subsection, we discuss the functioning of this new security scheme.

3.2 SBSS Operation

SBSS uses a different configuration file for each user, that ensures if a user is compromised, rest of the network will not be compromised with it. The configuration file contains the 256 slots and each slot is of 2-bits long. Thus for storing all slots in configuration file, we require only 2*256 bits.

3.2.1 Sending Phase

At the sender side first of all sender requires to select an algorithm and key for encryption/decryption. 2-bits codes for these four algorithms are randomly stored in the slots of slot structure. Slot is selected sequentially from slot structure. That means when SBSS runs for the first time, first slot of the slot structure is used and the algorithm corresponding to the 2 bits code in that slot is selected. When SBSS runs for second time, second slot of the slot structure is selected and so on. Keys are stored in key-lists and there are different key-lists for each algorithm. Keys are randomly selected from the key-list of the selected algorithm. Once a key is used from a key-list, it will be marked in that key-list so that it would not be used again.

Each node encrypts the new payload with the selected algorithm and key. The node appends SS, KS and all fields of data packet except data payload as a header to message as shown in figure - 3 and then sends the message.

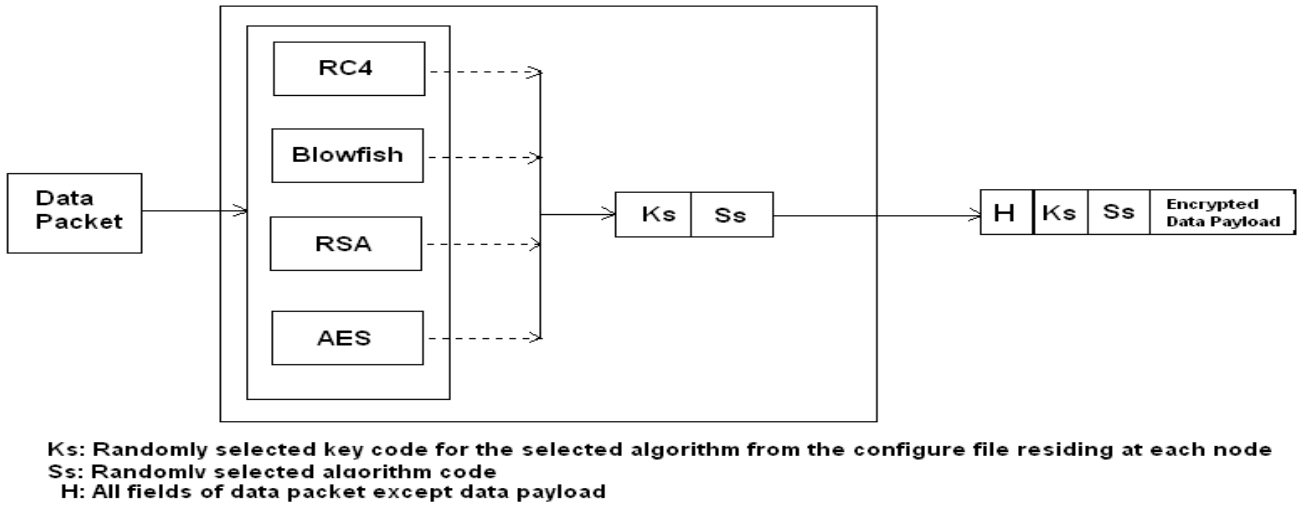

Figure 3. Data encryption in SBSS at source end

3.2.2 Receiving Phase

At the receiver side, receiver separates the SS, KS and encrypted data payload from the received packet. Receiver sends control packet to access point to know the exact algorithm and key corresponding to SS and KS fields of the received packet. The receiver uses selected algorithm and the key to decrypt the message.

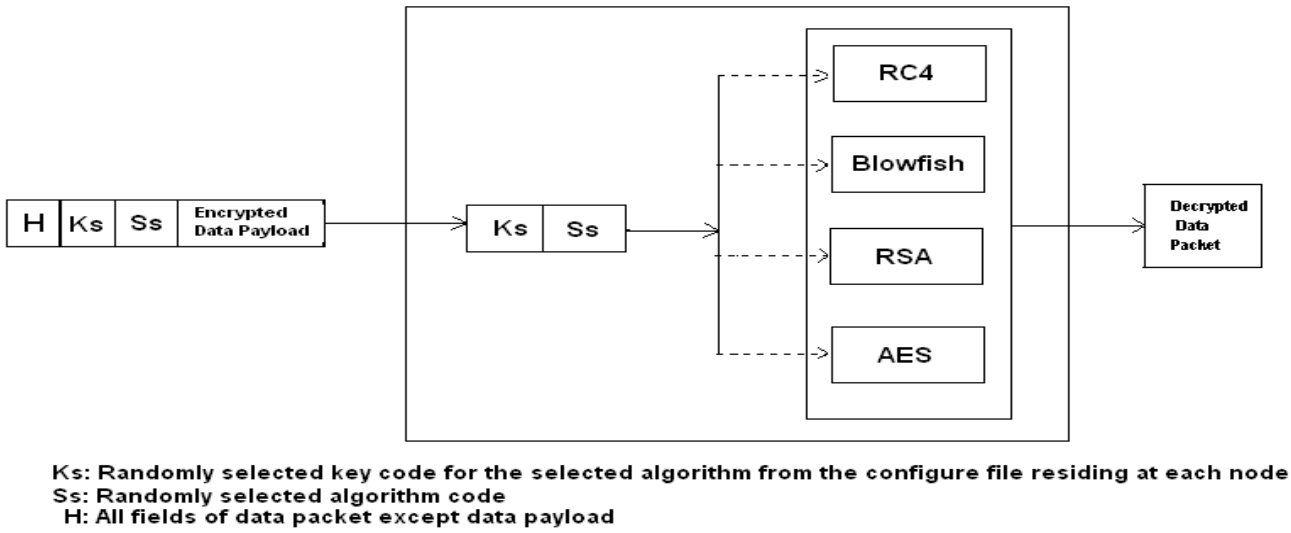

Figure 4. Data decryption in SBSS at destination end

3.2.3 AP Working

We assume that Access Point (AP) has powerful processing capability to handle various conversions and holds the powerful memory to store various files. The access point (AP) contains all the configuration files for all users and four key-lists files, one for each of four algorithms. It handles the decryption and the re-encryption of the transferred messages regarding getting information of key and selected algorithm from key-lists and configuration file of a user. AP acts more like a conversion server. Also, it has the authority to issue a refresh configuration file(s) and/or key-list(s) for node(s). When a node requires refreshing its configuration file and/or key-list(s), it will send a re-issue control packet to the AP. AP delivers it to the SBSS control server. The SBSS control server issues new files and/or key-list(s) and sends them to AP. AP keeps a copy of the files for itself and sends a copy to that node. The node receives the configuration file and/or key-list(s) and issues a control packet for acknowledgement to AP. AP replaces the old configuration file and/or key-list(s) with new one. The node also replaces the old configuration file and/or key-list(s) with the new one and resets all the counters.

Now we discuss the comparison among WEP, WAP2 and SBSS in table 1. In next section, we analyze the security scheme over different securities over the wireless networks performances.

Table 1 : Comparison between WEP, WPA2 and SBSS

Remarks	WEP	WPA2	SBSS
Time attack for single Packet using Brute force	2^{104} permutations	2^{128} permutations	$2^{RSA}+^{2Blowfish}+2^{AES}+2^{RC4}$ keys
Maintainability	NO	NO	YES
Execution Time	Less	more	Almost same as WPA2 (For large network lesser than WPA2)
Overall Security	Not Secure	Moderate Secure	High Level Security

4. SIMULATIONS

The objective of this section is to determine the overhead associated with IEEE 802.11 security protocols. More security is required on wireless networks to ensure reliability and data integrity. Applications associated with the use of wireless networks are continually expanding, and they could be impacted by slow response times or reduced throughput. Wireless bridges that connect campus buildings are currently capped at IEEE 802.11g speeds of 54 Mbps that is already much lower than typical gigabit wired solutions. The addition of encryption can only further hamper throughput on these links, independent of the fact that many users could be authenticating over the links as well.

Although not all of these issues are directly addressed in this paper, it should help to develop the need for a thorough understanding of the effects that security could cause on various types of network performance. As such the paper intends to provide general overviews of the current security protocols in use today and detailed description of our proposed security mechanism for wireless local area network; and how they compare to one another with respect to response time, latency, and throughput.

To conduct these experiments we have developed our simulator in C++ [14]. It involves the physical layer implementations of 802.11b and 802.11g with available MAC layer configuration and possible theoretical data rates specified by IEEE. The security protocols that we have implemented in this simulation include WEP, WPA and WPA2 and proposed method SBSS. There is also a "No Security" option available network types.

4.1 Parameters

We have evaluated 802.1lb and 802.llg networks with the security protocols that we have described in the previous sections. The performance measurements of our simulation are total simulation time, throughput, packet delivery fraction and average end-end packet delivery fraction. We have also measured Total Simulation Time Distribution and throughput for 20 and 50 nodes at different data rates.

In our simulation, we have taken the following parameters:
Number of Nodes: 10, 20,30,40,50 and 60 nodes
Packet Length Distribution: Constant
Data Rates: 6,12,36,48 and 54 Mbps
Security Mechanisms: No Security, WEP with 104 bit Key, WPA, WPA2 (802.11i)and SBSS.

4.2 Network Performance Metrics

As mentioned above the paper focuses on various metrics related to network performance. Because these performance metrics comprise the bulk of the data presented in the paper, it is important to understand them and how they can be measured accurately.

4.2.1 Metric Descriptions

There are a large number of performance metrics that network engineers utilize to analyze network configurations and troubleshoot problems. The ones most commonly referred to are throughput and latency, but there are more depending on the media that the network exists within. The following is a brief overview of some performance metrics commonly used today:

• Throughput – "A measurement of the data-transfer rate through a complex communications or networking scheme." It is important to note that throughput is a measurement of a certain amount of data through a link over a given time and can be affected by processor and disk performance, operating system capabilities, network hardware limitations, and the amount of data being transmitted.

• Latency – "The time delay involved in moving data traffic through a network". The three sources of latency are propagation delay, that is caused by the time necessary for data to travel the length of the link; transmission delay, that is the actual time necessary for data to be moved across the network; and processing delay, that is the time needed for data encapsulation and route establishment.

• Evaluating average End-to-End packet delivery time -For each packet we calculate the send (s) time (t) and the receive (r) time (t) and average it.

. Packet Delivery Fraction - As the Packet Delivery Fraction (PDF) is the ratio between the number of data packets received and those sent by the sources it is necessary to calculate the number of sent and received packets from the traces.

These are just a few of the many terms used to analyze the performance of networks, but are the only ones referred to in this paper.

5. RESULTS

In our simulation, we have evaluated several configurations for 802.11b and 802.11g networks and obtained several performance values. Here, we are highlighting the comparison between our security mechanism SBSS and previous the most secure security mechanism WPA2 in WLAN on the basis of various network performance metrics.

The following figures from 5 to 10 show some of the interesting results of our evaluation using simulator.

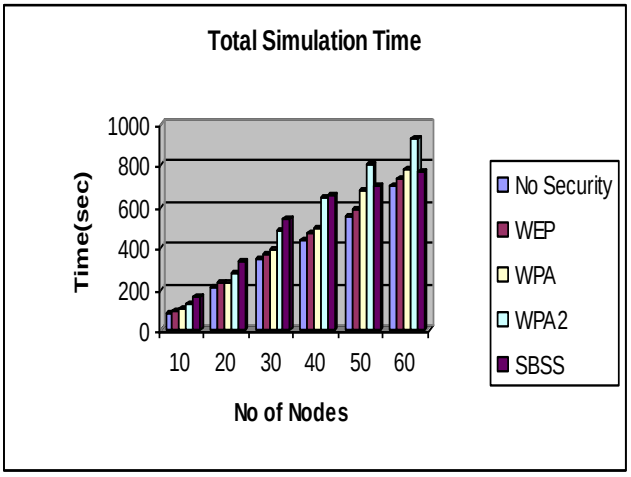

Figure 5 Total Simulation Time - (Number of Nodes)

Figure 5 shows the effect of number of nodes in the network on total simulation time in no security and with security network structures. Total simulation time is the time that is required to send a particular number of packets by a particular number of nodes to destination node with respective security mechanism. It shows that as the number of nodes in the network increases, the total operating time of the network also increases. When number of nodes in the network is less, total operating time for our proposed security mechanism (SBSS) is almost same as previous most secure mechanism WPA2. But on increasing the number of nodes in the network, total simulation time of SBSS drastically decreases in comparison to WPA2.

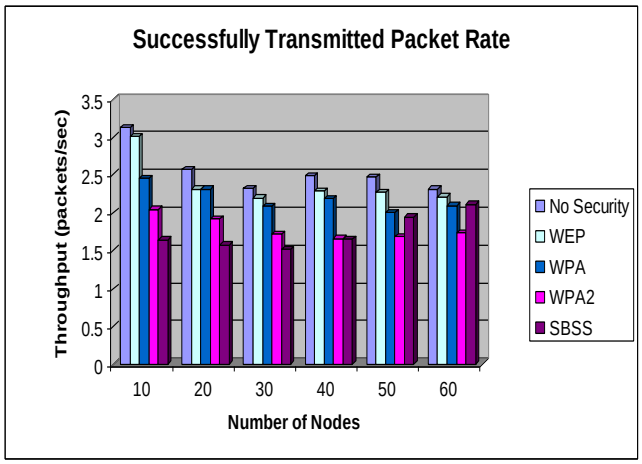

Figure 6 Successfully Transmitted Packet Rate for 802.11b (11 Mbps)

Figure 6 shows the successfully transmitted packet rate with respect to the number of nodes in the network. This graph shows that if number of nodes is very less, throughput of our security mechanism (SBSS) is somewhat lesser than the pervious secure mechanism WPA2. With the increase in number of nodes in the network, the difference between throughputs of WPA2 and SBSS goes on to decease. Moreover, more increase in the number of nodes in the network also increases the throughput of our security mechanism (SBSS) in comparison to previous secure mechanism WPA2.

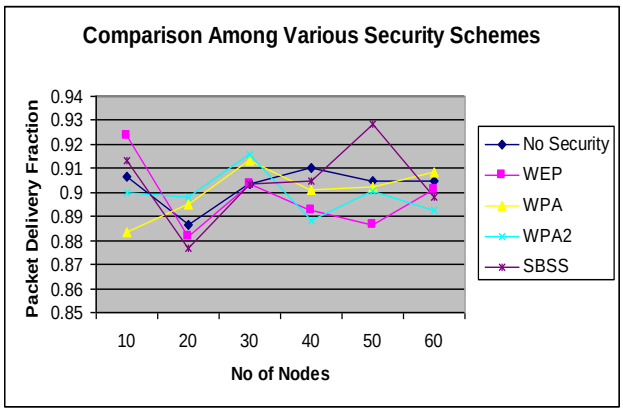

Figure 7 Packet Delivery Fraction for various security mechanisms

Figure 7 shows the packet delivery fraction with respect to the number of nodes for various security mechanisms. Packet drop for each security mechanism depends on channel drop rate. Figure 7 shows that packet delivery fraction for our proposed security mechanism SBSS is almost same as previous security mechanisms.

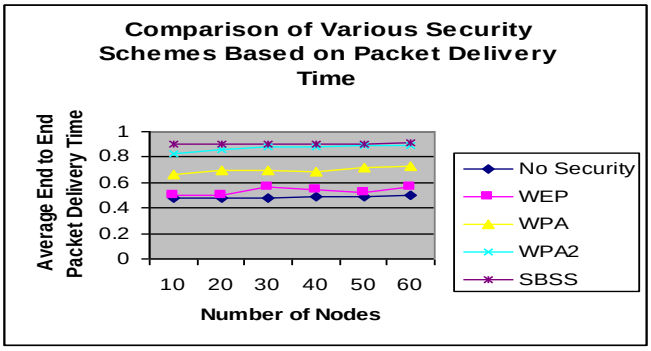

Figure 8. Average End to End Packet Delivery for various security mechanisms

Figure 8 shows that when the network is getting more and more crowded, adding security features increases the packet delay and drop rate, thus decreases the network performance. Packet delay for our proposed security mechanism SBSS is almost same as WPA2. For example, for 50 and 60 number of nodes, there is no difference between the average end to end packet delivery times of SBSS and WPA2.

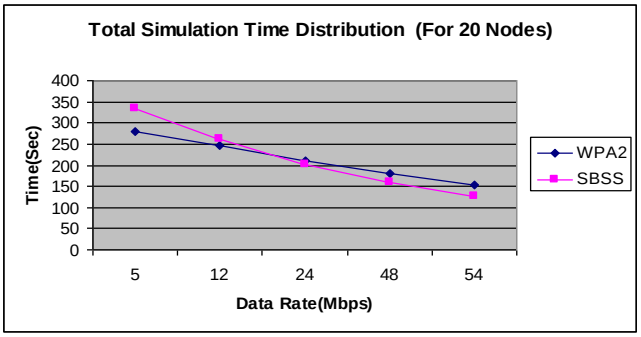

Figure 9. Data Rate - Time graph for different security mechanisms in 20 nodular 802.11g networks

Figure 9 shows the performance of 20 nodular 802.11g network structures in terms of total simulation time and different data rates. Figure 9 shows that increase in data rate results decrease in the total simulation time. Figure 9 concludes that at less data rates total simulation time for SBSS is more than WPA2 but at higher data rates total simulation time for SBSS decreases in comparison to WPA2.

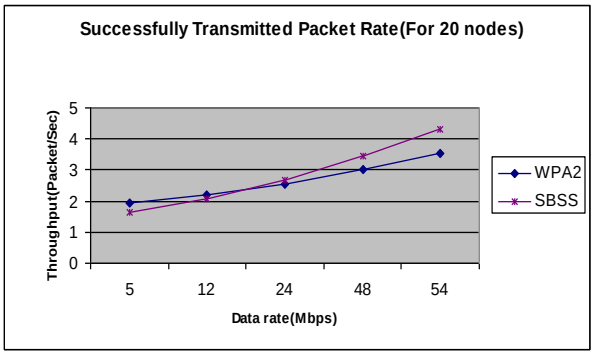

Figure 10. Successfully transmitted Packet Rate for 20 Nodes

Figure 10 shows the performance of 20 nodular 802.11g network structures in terms of successfully transmitted Packet Rate and different data rates. Figure 10 shows that at less data rates throughput for SBSS is less than WPA2 but at higher data rates throughput for SBSS increases rapidly in comparison to WPA2.

6. CONCLUSION

Simulation results presented in section 5 and analysis described in section 3 are encouraging in the sense that our proposed security protocol SBSS is highly efficient as it provides an drastic increase in security with almost same overhead on network performance as exiting most secure protocol in WLANs. In this paper, we have analyzed the performance of wireless local area networks (WLANs) and security strength of standard security protocols available in WLANs and their overhead as performance concern. These available security mechanisms are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and WPA2. Each existing security protocol in WLAN has various vulnerabilities as described in section 2. Among these existing security protocols in WLANs, WPA2 is the most secure security protocol but trade-off between security and overhead associated with it is not good. To counter all these problems, this work provides an in-depth look into the description of our proposed security mechanism Slot based security scheme (SBSS) in WLANs. SBSS counters all the vulnerabilities in the existing security protocols in WLANs and results a good trade-off between security and overhead associated with it on network performance

We have simulated these security schemes in c++ with certain parameters. We have concluded that when the number of nodes is less in the network, the security features do not affect the network performance very much. The simulation results described for the throughput and simulation time for large number of nodes show the clear pattern about the efficiency of our proposed security scheme over existing security mechanisms for wireless networks.

By using not only one but four algorithms to encrypt and decrypt, any hacker or intruder needs to devise a mean to guess the exact slots configurations for each node in the network. The time factor of SBSS does not depend only on the key but also depends on the combinations of the keys along with the possible combinations of the slots.

7. REFERENCES

[1] Wi-Fi Alliance. “Wi-Fi Protected Access (WPA) version 3.1”. August 2004.

[2] A. Mishra and W. Arbaugh, “An Initial Security Analysis of the IEEE 802.1X Standard”, http://www.cs.umd.edu/~waa/1x.pdf, February 2002

[3] Issues in Wireless Security (WEP, WPA & 802.11i) Presented to the 18 th Annual Computer Security Applications Conference 11 December 2002 Brian R. Miller, Booz Allen Hamilton

[4] Introduction to 802.1X for Wireless Local Area Networks,2002, Interlink Networks www.interlinknetworks.com

[5] WPA: A Key Step Forward in Enterpriser-class Wireless LAN (WLAN) Security, Jon A. LaRosa, MeetingHouse data communications, 2003

[6] Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks, Wi-Fi Alliance, 2003 www.weca.net5

[7] 802.11 Security Series Part II: The Temporal Key Integrity Protocol (TKIP), Jesse Walker, Intel Corporation, 2002

[8] The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards Stanley Wong GSEC Practical v1.4b, 2003

[9] J.Daemen and V.Rijmen "AES Proposal: Rijndael," 1998.

[10] NEW PROTOCOL DESIGN FOR WIRELESS NETWORKS SECURITY Prof. Dr. Gamal Selim, Cairo, Egypt

[11] IEEE Standards Association, IEEE 802.11 speci_cations. Technical speci_cations, 1999-2004. http://standards.ieee.org/getieee802/802.11.html

[12] S. Gayal and S. A. Vetha Manickam, Wireless LAN Security Today and Tomorrow. Pune, India: Center for Information and Network Security, Pune University, 2002.

[13] IEEE 802.11 Working Group, Task Group I IEEE 802.11 Wireless LAN Standards, 2004 [Online]. Available: http://grouper.ieee.org/groups/802/11

[14] B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C. New York: Wiley, 1996, pp. 397–398.

[15] Original posting of RC4 Algorithm to Cypherpunks mailing list 2006 [Online]. Available: http:// cypherpunks.venona.com/archive/1994/09/msg00304.html

[16] AES (Rijndael) Specification and Information National Institute of Standards and Technology, Boulder, CO, 2004 [Online]. Available:http://csrc.nist.gov/encryption/aes/rijndael