

Improving Data Transmission security in a Wireless Network Using Digital Signature

¹Aniekwe V. N., ²Ufoaroh S.U., and ³Alumona T.L

¹ Masters Candidate, Department of Electronic and Computer Engineering, Faculty of Engineering, Nnamdi Azikiwe University, Awka, Anambra State.

^{2,3} Senior lecturers, Department of Electronic and Computer Engineering, Faculty of Engineering, Nnamdi Azikiwe University, Awka, Anambra State.

¹viviananiekwe@gmail.com

²sufoaroh@yahoo.com

³tl.alumona@unizik.edu.ng

Abstract-This thesis is aimed at improving the data transmission security in wireless network. The widespread proliferation of computer networks has resulted in the increase of attacks on information systems. These attacks are used for illegally gaining access to unauthorized information, misuse of information or to reduce the availability of the information to authorized users. This results in huge financial losses to companies and can also result in losing their goodwill to customers and services are severally disrupted. So, this thesis is designed to improve the data transmission security in wireless network. The data network under study was characterized to find out the performance of the parameters of the network. The packet loss was evaluated and a modified digital signature algorithm was developed. The thesis also simulates the Network Activity Tracking using digital Signature using php-mysql model. With the modified digital signature algorithm the network security was improved resulting to less packet delivery response time on the data network as the minimum packet delivery time recorded was 1.2 seconds in different simulations time which is less when compared to the earlier measurement when digital signature was not used and we obtained minimum packet delivery time recorded of 20 seconds. This shows a reduction in minimum packet delivery time of 18.8 seconds which is a great improvement in data delivery rate in network. This improvement can reduce data loss due to network delay and improve the security in the network.

Keywords: Algorithm, Data Encryption, Data Transmission, Digital Signature, Network Security, Nodes, Wireless Network

1.0 Introduction

In this computer age, most organizations and individuals are highly conducting transactions via the internet and this has left all day to day activities highly depending on information communication technology. With this, the use of internet is growing at an exponential rate in the last decades and continues to develop in terms of dimension and complexity (Gupta, 2010). With

the increase of distributed systems and data telecommunication networks, the need for automated security tools for protecting data and information became an essential requirement. Many of the data stream applications operate over Internet and/or wireless communication networks and are thus exposed to numerous threats such as:

- Attacks on data integrity: data can be injected or modified and it is not in the original form as intended by the sender, or originally stored. Data corruption can be due to faults as well as to malicious actions.
- Attacks on data confidentiality and privacy: by eavesdropping of communications channels, or bypassing the access control and authorization mechanisms, or by inferring information from data they have legitimate access to, attackers can obtain either access to, or learn private information (Farkas, 2012).
- Attacks on data validity: malicious clients can inject or update corrupted packets that can potentially compromise the accuracy of query answers on a stream or set of streams. Such attacks are extremely difficult to defend against and potential solutions require corroborate information from multiple independent sources and often depend on application semantics.
- Denial of service: attackers can exhaust either the available bandwidth or the database server resources, preventing legitimate clients from obtaining service. At the extreme, such attacks can render the system unavailable.

Also, with the advancement of computer technology and the wide spread use of computer networks, the security of internal network against attacks, illegitimate traffics and unauthorized access can be crucial to the success of the entire business operation.

The goal of this research work is to highlight the challenges posed by the vision of a global hotspot infrastructure, and discuss the research problems that remain to realize this vision. In this research work a hybrid security measures that will involve encryption and digital signature technique for the purpose of maintaining a secured packet transmission in a wireless data communication network. In this, to detect the malicious node in network digital signatures are used. Digital signature is one of the verification techniques. All nodes have legitimate digital signature. The route request is send to neighbor nodes by the source node. If destination node is one of them then ok, otherwise route request broadcast to next node until the destination is found. The route request (RREQ) packet header contains the information of visiting node (node-

id) in node information column and hop count column which contains the number of visiting nodes used in path. The destination node selects the shortest path with minimum number of nodes. the destination node unicast the reply whose header contain the column of node-id that contains the id of all nodes used in that path and digital signature column in which each visiting node adds its digital signature. When the receiving node receives packet, it compare the digital signature of the previous node from its database. If the signature is match then that node is legitimate otherwise that node is considered as malicious node. When malicious node is detected then that info is broadcast to the neighbors. This process is repeated until the secure path is not found.

2.0 Review of Related Works

A lot of research was reviewed on the way to identify new threats and create secure mechanisms to counter those threats in a wireless network. From the literatures reviewed, it can be seen that in computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted. Firewalls impose restrictions on incoming and outgoing Network packets to and from private networks. Network firewalls filter traffic between two or more networks; they are either software appliances running on general purpose hardware, or hardware based appliances.

Table 1 summarizes some of the related studies, the techniques they adopted, the contribution and limitations of the studies.

Table 1: Summary of Past Related Studies

| Authors | Technique Adopted | Contribution | Limitations |
|-----------------------|---------------------------------|--|---|
| Langendoerfer, (2017) | firewall management plane (FMP) | It checks if the packet belongs to an existing connection and if the source address is already blocked | The approach cannot detect whether an incoming packet is malicious or not |

| | | | |
|-------------------|--|---|---|
| Pranschke, (2009) | automated firewall rule set generation | solved time wastage which was faced when creating rule sets | useful rule sets can be neglected |
| Rosselti (2011) | integrate security architecture for WAN | The work try to eliminate unavailable or disrupt the connection between legitimate peers | Still leaves some loop holes for network attack |
| Matsunage (2012) | 4-way handshake algorithm | Tries to ward-off intruders | Prevents network intrusion only |
| Owen (2014) | wireless intrusion detection response system | The work has 3 phase of operation in managing network security (network discovery, authentication and key generation distribution). | Prevent only session hijacking threat. |
| Borisov (2014) | intercepting intruders in mobile communication | The work try to prevent adversary that are capable of doing message deletion | This approach cannot identify and prevent more attacks so it is not a robust approach |
| Lee (2015) | multipath approach | the approach identify legitimate message transaction between the supplicant, authenticator and authentication server | It can give false alarm |
| Bsufka (2016) | combination of firewalls, antivirus monitoring tools and IDS | can detect packets on the network | negative and positive false alarms can be generated and genuine packets can be denied |

Though the method used is different from the existing traditional firewall, more studies are required to fully work on the challenges of traditional firewall. Method of an intelligent agent based early warning system (A-EWS) as proposed in this research work aimed at detecting any attacks or intrusions on a network as early as possible. By using IDS successfully managed to

detect any attacks or intrusions on a network as early as possible. The Research Gap Identified is that Most of the work reviewed has shown that there are still some major weaknesses on the technique they adopted. The techniques they applied in Bsufka (2016) shows that negative and positive false alarms can be generated and genuine packets can be denied and this leaves some loop holes for network attack which is a major research gap. Thus, eliminating wireless security threats by augmenting the network with digital signature technique provides strong confidentiality, integrity and replay protection for easy transmitted message in a data network.

3.0 Research Methodology

The research work proposed to improve data transmission security in wireless data network using digital signature. Digital signature is the one of the verification technique. The certification process in an asymmetric key algorithm depends on digital signatures to provide trust. A digital signature is an electronic method of signing an electronic document that is reliable, convenient and secure. A digital signature mechanism consists of a digital signature generation and associated digital signature verification. A simplistic model of digital signature schemes involves a sign operation that uses a sender's private key to generate a signature. The receiver retrieves the sender's certified public key from a Certificate Authority (CA) and performs a verify operation on the signature. A successful verification procedure convinces the receiver that the received message is from the actual originator and the contents are not tampered since leaving the originator.

The methodology used is a two step process; Embedding Process and Restoration Process. The Embedding Process follows the sequence bellow and is depicted in figure 3.1.

- 1) In this process Company information like-Name, address and phone are stored in the text file data.txt.
- 2) Compute the hash of the data information.
- 3) This hash is encrypted with the private key of the sender and digital signature is then generated. The key generation is based on RSA Algorithm. RSA is a public key crypto-system having two keys-Public Key and the Private Key.
- 4) The digitally signed information is encoded into the Quick Response (QR) Code.
- 5) The secured code is then embedded in an image to form the watermarked image.

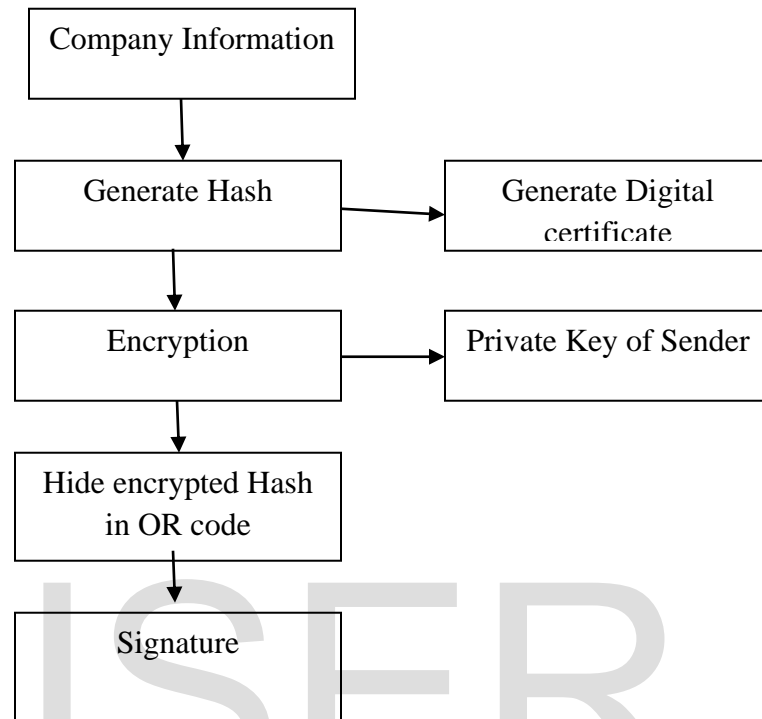


Figure 1: Flowchart of Embedding Process for the digital signature

In the restoration process we apply the extraction process scheme and extract the encrypted QR Code following the steps below and as shown in figure 3.2.

1. To decode the QR Code any QR code decoder can be used and encrypted hash of the company information is obtained.
2. To recover the original company information it is decrypted by using the public key and the digital signature.
3. If some different QR code is decrypted, then this information will not match and it is rejected.
4. Or if the hash is not matched, then also it will be rejected confirming that the sender is not authentic and the image has been tampered.

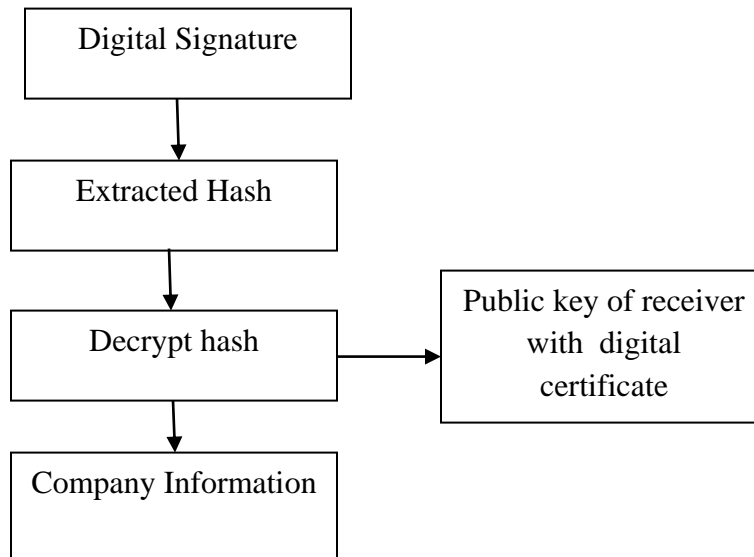


Figure 2: Flowchart of Restoration Process for the digital signature

3.2 Digital Signature Algorithm

Let p and q be primes so that q divides $p - 1$,

h a positive integer less than p , and $g = h^{(p-1)/q} \bmod p$.

Then $g^q \bmod p = 1$, and if $m \bmod q = n \bmod q$, then $g^m \bmod p = g^n \bmod p$.

Proof: We have

$$g^q \bmod p = (h^{(p-1)/q} \bmod p)^q \bmod p$$

$$= h^{(p-1)} \bmod p$$

$$= 1$$

Now let $m \bmod q = n \bmod q$, i.e.,

$$m = n + kq \text{ for some integer } k.$$

Then $gm \bmod p = gn+kq \bmod p$

$$= (gn \bmod p) (gkq \bmod p)$$

$$= ((gn \bmod p) (gq \bmod p)^k) \bmod p$$

$$= gn \bmod p$$

Since $gq \bmod p = 1$.

We are now ready to prove the main result.

THEOREM. If $M' = M$, $r' = r$, and $s' = s$ in the signature verification, then $v = r'$. Proof: We have

$$w = (s')^{-1} \bmod q = s^{-1} \bmod q$$

$$u1 = ((\text{SHA-1}(M'))^w) \bmod q = ((\text{SHA-1}(M))^w) \bmod q$$

$$u2 = ((r')^w) \bmod q = (r^w) \bmod q.$$

Now $y = gx \bmod p$, so that $v = ((gu1 \bmod p) \bmod q)$

$$= ((g^{\text{SHA-1}(M)^w} y^{rw}) \bmod p) \bmod q$$

$$= ((g^{\text{SHA-1}(M)^w} g^{xrw}) \bmod p) \bmod q$$

$$= ((g^{(\text{SHA-1}(M)+xr)^w}) \bmod p) \bmod q.$$

Also $s = (k^{-1}(\text{SHA-1}(M) + xr)) \bmod q$, Hence $w = (k(\text{SHA-1}(M) + xr)^{-1}) \bmod q$

$(\text{SHA-1}(M) + xr)^w \bmod q = k \bmod q$. Thus $v = (gk \bmod p) \bmod q = r$

3.3 Model for Data Transmission Network Using Digital Signature

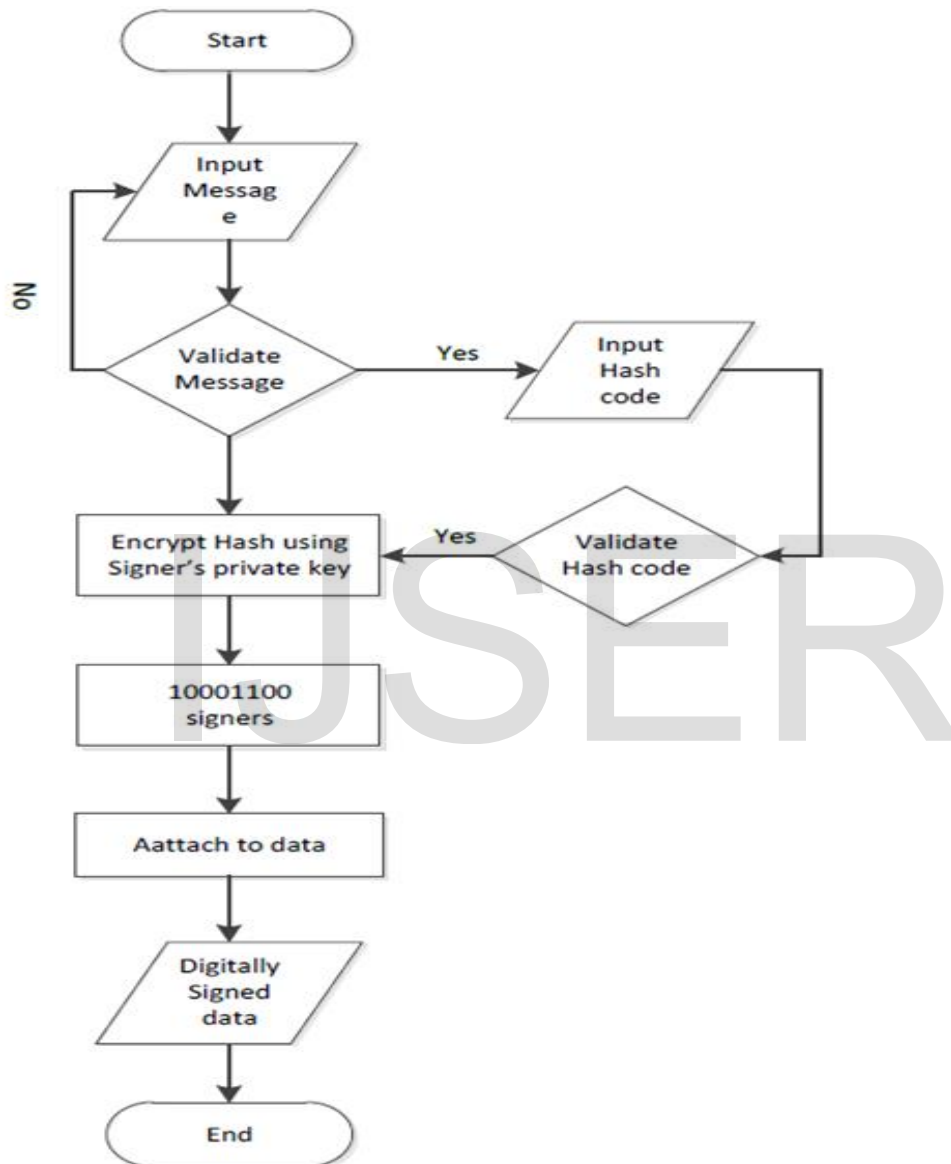


Figure 3: Flowchart for Encryption with Digital Signature

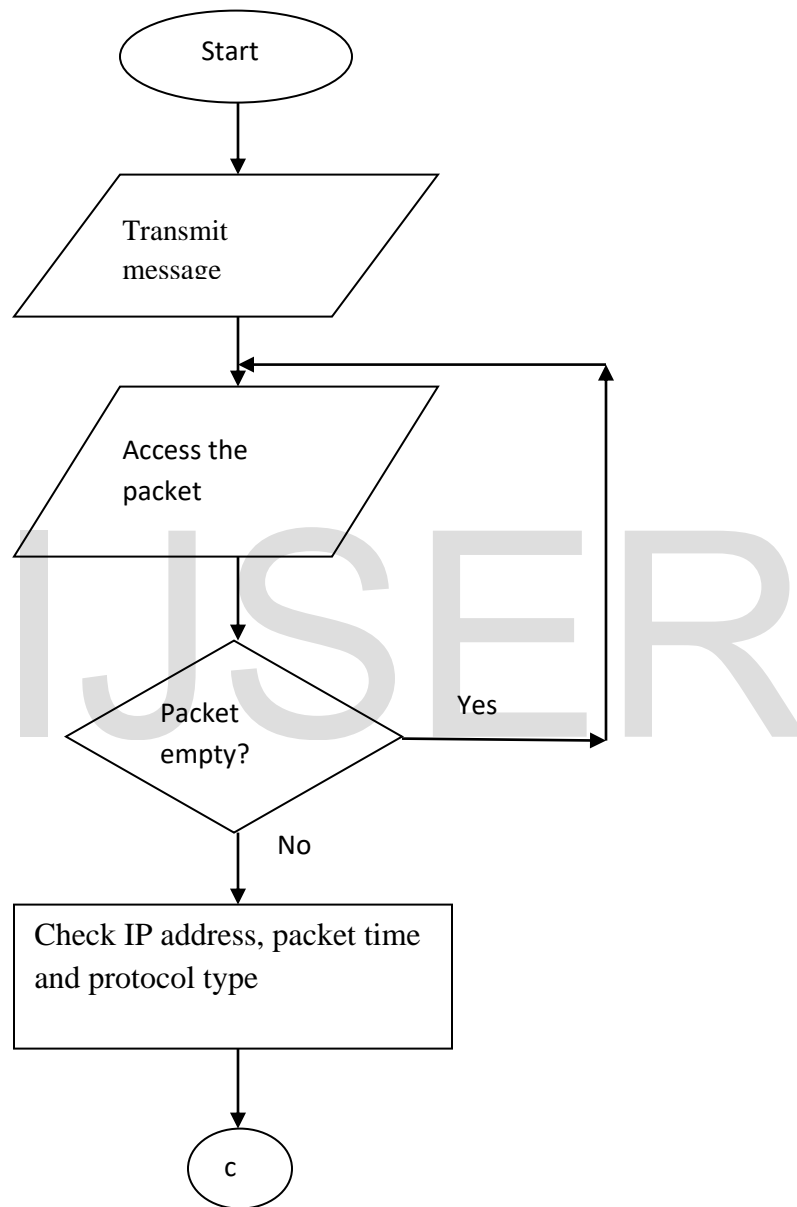


Figure 4: Flowchart for Network Authentication

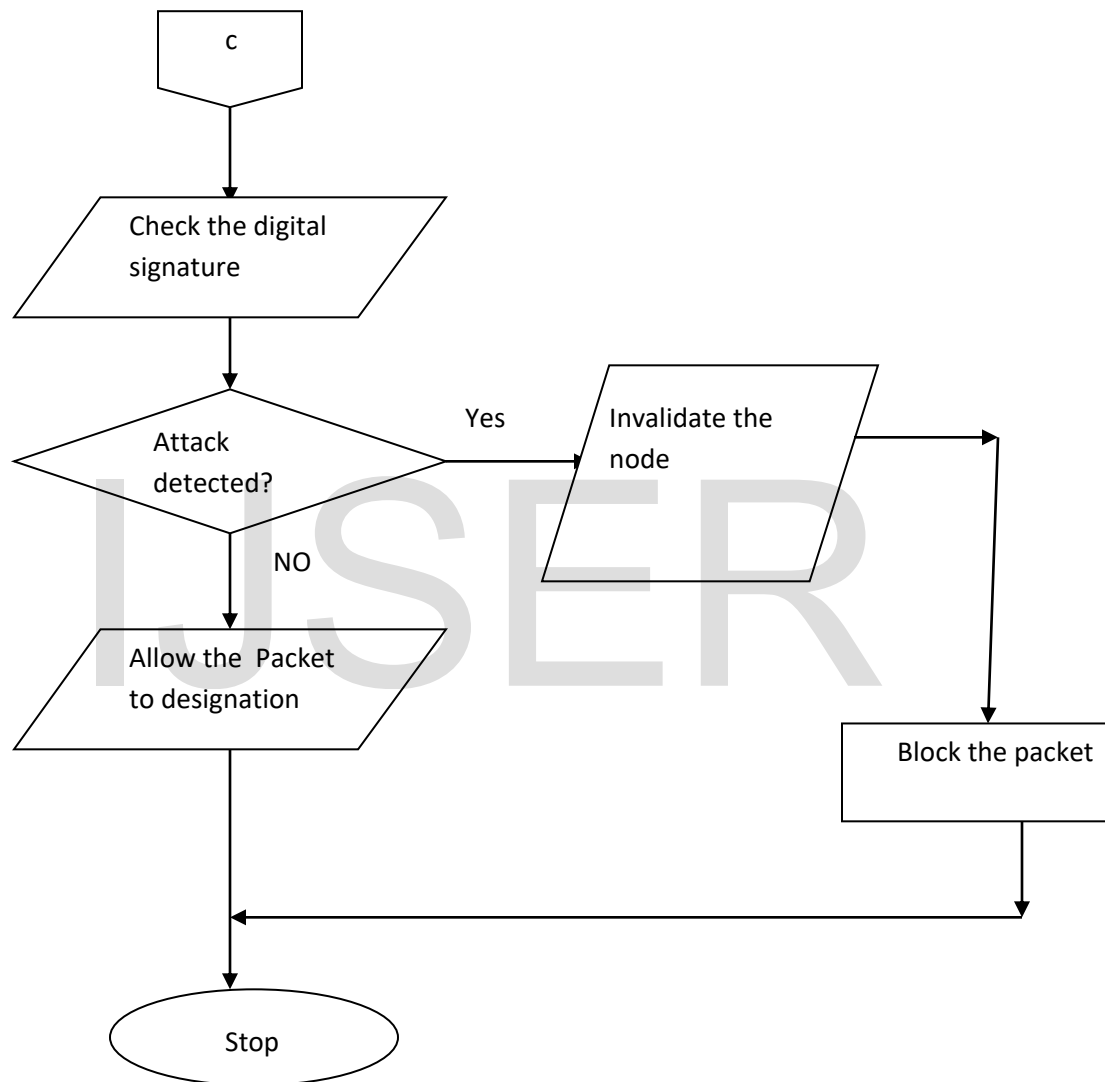


Figure 5: Flowchart for network authentication

4.1 Simulation Result

This chapter provides a detailed description about the results and analysis of the obtained data. For data transmission each host transmits a Packet to its neighbor nodes. When data pass from one node to another node, every node signs the data so that the receiver node can get the message by this same signature. The sender node signs the information by its public key and encrypts the data. The encrypted data passes to the neighboring node. Here, hash chain is used in such a suitable system so that the data pass rate of the digital remains high. The design interface for data transmission on the network is as shown in figure ,6 7, 8, and 9.

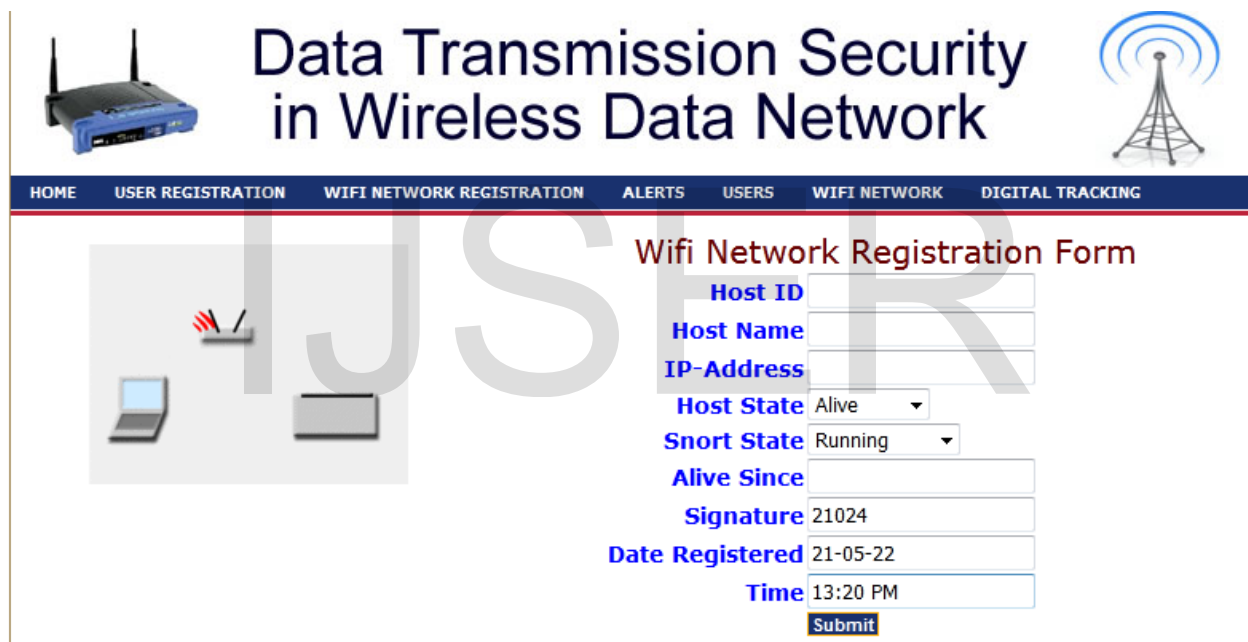


Figure 6: Network Setup form

This form is used to register nodes on the network for the purpose of assigning a digital signature to the network point. Only nodes with digital signature can transmit data on the network.

Alerts Report

| Host Id | Alert Id | Time Stamp | Rules Id | Alert Message | Action |
|---------|----------|---------------------|----------|--|-------------------|
| 1100 | 1 | 2021-05-22 11:41:21 | 1002 | Agent Authenticated Successful | Allow Access |
| 1100 | 2 | 2021-05-22 11:54:21 | 1002 | Agent Authenticated Successful | Allow Access |
| 1100 | 3 | 2021-05-22 11:54:34 | 1002 | Agent Authenticated Successful | Allow Access |
| 1100 | 4 | 2021-05-22 11:55:01 | 1007 | Invalid Network User | Upload Denied |
| 1100 | 5 | 2021-05-22 11:59:31 | 1007 | File Uploaded | Upload Successful |
| 1100 | 6 | 2021-05-22 12:00:09 | 1010 | Open the mail inbox | Mails Read |
| 1100 | 7 | 2021-05-22 12:00:53 | 1010 | Message sent to citysoft2010@yahoo.com | Mail Delivered |

Mails Outbox Report

| Host Id | Time Stamp | Send To | Message |
|---------|---------------------|------------------------|--|
| 1100 | 2021-05-12 10:08:30 | citysoft2010@yahoo.com | Hi, When are you coming to inspect the goods |
| 1100 | 2021-05-20 10:39:42 | jef@yahoo.com | Yes i killed him |
| 1100 | 2021-05-20 10:48:10 | jef@yahoo.com | When is the balance coming |
| 1100 | 2021-05-22 12:00:53 | citysoft2010@yahoo.com | How are you doing |

Mails Inbox Report

| Host Id | Time Stamp | Send From | Message |
|---------|---------------------|------------|---------------------------------------|
| 700 | 2021-05-16 10:26:55 | Mark Jefry | I will send the money by 2pm tomorrow |
| 700 | 2021-05-16 10:27:21 | Mark Jefry | Did you kill the бага |

Recoverd Files

| Host Id | Time Stamp | Send From / To | Message |
|---------|---------------------|----------------|-----------------------|
| 700 | 2021-05-16 10:27:21 | Mark Jefry | Did you kill the бага |
| 1100 | 2021-05-20 10:39:42 | Herry Onyia | Yes i killed him |

File Upload Report

| Host Id | Time Stamp | File Name |
|---------|---------------------|--------------------------------------|
| 1100 | 2021-05-17 12:13:29 | Open File Click here |
| 1100 | 2021-05-18 12:14:24 | Open File Click here |

Figure 7: Network Activity Tracking using digital Signature.

Figure 7 shows network users activity and system respond to each data transmission made. The system uses the digital signature to track all activities on the network and relate it to the network users.

| Alerts Report | | | | | |
|---------------|----------|---------------------|----------|---|-------------------|
| Host Id | Alert Id | Time Stamp | Rules Id | Alert Message | Action |
| 1100 | 1 | 2021-05-22 11:41:21 | 1002 | Agent Authenticated Successful | Allow Access |
| 1100 | 2 | 2021-05-22 11:54:21 | 1002 | Agent Authenticated Successful | Allow Access |
| 1100 | 3 | 2021-05-22 11:54:34 | 1002 | Agent Authenticated Successful | Allow Access |
| 1100 | 4 | 2021-05-22 11:55:01 | 1007 | Invalid Network User | Upload Denied |
| 1100 | 5 | 2021-05-22 11:59:31 | 1007 | File Uploaded | Upload Successful |
| 1100 | 6 | 2021-05-22 12:00:09 | 1010 | Open the mail inbox | Mails Read |
| 1100 | 7 | 2021-05-22 12:00:53 | 1010 | Message sent to citysoft2010@yahoo.com | Mail Delivered |
| 700 | 9 | 2021-05-22 12:04:24 | 1002 | Agent Authenticated Successful | Allow Access |
| 700 | 10 | 2021-05-22 12:06:15 | 1007 | Buffer Overflow | Upload Denied |
| 700 | 11 | 2021-05-22 12:06:51 | 1007 | Invalid Network User | Upload Denied |
| 700 | 12 | 2021-05-22 12:07:26 | 1007 | Invalid Network User | Upload Denied |
| 700 | 13 | 2021-05-22 12:08:18 | 1007 | File Uploaded | Upload Successful |
| 700 | 14 | 2021-05-22 12:08:25 | 1010 | Open the mail inbox | Mails Read |
| 700 | 15 | 2021-05-22 12:08:33 | 1010 | Selected a Mail | Mails Deleted |
| 700 | 16 | 2021-05-22 12:09:14 | 1002 | Agent Authenticated Successful | Allow Access |
| 0 | 21 | 2021-05-22 12:32:09 | 1001 | Agent State changed to un-authenticated | Block |
| 0 | 22 | 2021-05-22 12:35:50 | 1001 | Attempted Admin Privillages | Block |
| 0 | 23 | 2021-05-22 12:38:20 | 1001 | Attempted Admin Privillages | Block |
| 700 | 24 | 2021-05-22 12:39:43 | 1002 | Agent Authenticated Successfully | Access Allowed |

Figure 8: Network Monitoring

The network monitoring and alert shows the response of the data network to user's request. It is log file that shows whether data transmission was successful or failed and it shows the action taken by the system at each request.



Data Transmission Security in Wireless Data Network



[HOME](#)
[HOST](#)
[ALERTS](#)
[SEND REQUEST](#)
[SEND MAIL](#)
[READ MAIL](#)
[LOG OUT](#)

Connect to Wifi Network and Upload Packets

Select File to Upload

 No file selected.

Enter the Digital Signature

File Size : byte(s)

Figure 9: Data Transmission Interface

Figure 9 is the interface for transmitting data to the server. It allows users to upload data and the system verifies the digital signature before the action can be completed.

4.2 Performance Measurement

Performance testing is the testing to assess the speed and effectiveness of the system and to make sure it is generating results within a specified time as in performance requirements.

Table 2: Wireless Network Security Performance comparison

| Trials | Activities | Response time (seconds) without Digital Signature authentication | Response time (seconds) with Digital Signature authentication |
|---------------|--------------------|---|--|
| 1 | Access the network | 20 | 5 |
| 2 | Read mail | 20.22 | 5.22 |
| 3 | Send mail | 55.48 | 15 |
| 4 | Receive mail | 19.98 | 2.91 |
| 5 | Access network | 15.94 | 4.94 |
| 6 | Send mail | 19.81 | 12.81 |
| 7 | Upload file | 90.93 | 20.13 |
| 8 | Send mail | 49.79 | 3.72 |
| 9 | Read mail | 30.07 | 4 |
| 10 | Download file | 99.68 | 23 |
| 11 | Read mail | 23.9 | 2.2 |
| 12 | Access the network | 72.4 | 4 |
| 13 | Send mail | 45.1 | 4.5 |

| | | | |
|----|-----------|-------|-----|
| 14 | Read mail | 23.65 | 3 |
| 15 | Log out | 30 | 1.2 |

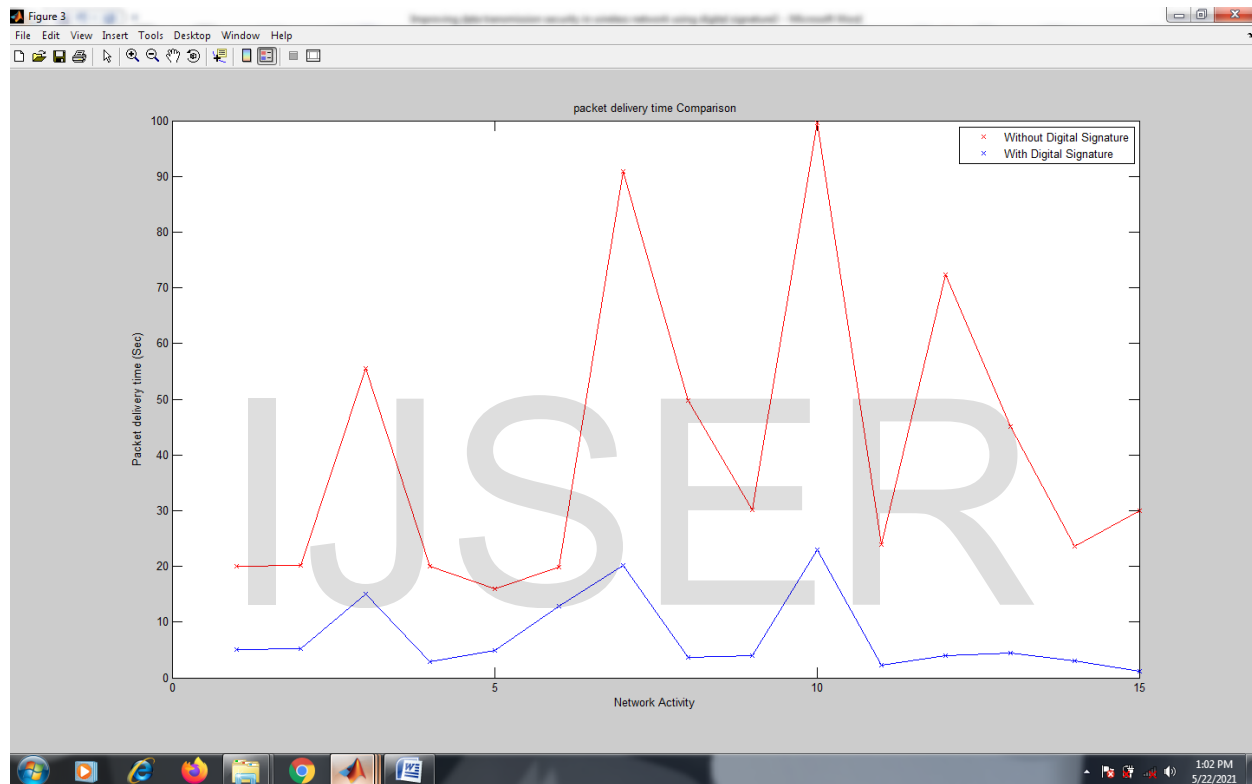


Figure 10: Comparison of Wireless network security Performance evaluation in terms of System Response time (seconds) with and without digital signature authentication

Figure 10 showed the simulation performance of the system response time at peak hour. The network speed was compared with and without digital signature authentication. Digital Signature authentication has a faster response time and resulted in reduction in packet delivery time. The minimum seconds used in the

activities under this condition is 1.2 seconds which is acceptable while that of un-authenticated network is 20 seconds.

5.0 Conclusion

In this project, it was proposed that authentication and key establishment in wireless networks using valid digital signature authentication id with key exchange sessions from the server. Wireless network introduction at the AP switches which connects the supplicants to the server have addressed some inherent weakness in wireless networks. This work have identified and analyzed weaknesses in previous security schemes for wireless networks, and proposed the authentication model which uses digital signature to improve security in wireless networks. The proposed model, each client shares an independent password and digital signature for the node with a trusted server for authentication and access control. Hence the new system provides for great efficiency in both computation and communications in wireless networks as shown in the performance evaluations.

ACKNOWLEDGMENT

The Authors wish to thank the Almighty God who is the source of all knowledge, Aniekwe Chukwunonso (ESQ), Dr. Alumona T.L, Dr. Nobert Okwara. This work was fully supported by a grant from Aniekwe Chukwunonso (ESQ). May God richly bless you all Amen.

References

- Al-Shaer, E. and Hamed, H. (2016) "Discovery of policy anomalies in distributed firewalls", in Proc. IEEE INFOCOM, Mar. 2016, pp. 2605–2616.
- Acharya, S., Wang, J. and Ge, Z (2016) "Simulation study of firewalls to aid improved performance," in *Proc. 39th Annual Symposium on Simulation*, USA, Apr. 2-6, 2016, pp. 18-26.
- Ahuja, H. and Gupta, E. J. (2012) "Analysis of Malicious Data in Underwater Sensor Network," International Journal of Engineering Research and Applications, vol. 2, no. 4, pp. 967-971
- Alfantookh, A. A. (2016) "DoS attacks intelligent detection using neural networks," Journal of King Saud University- Computer and Information Sciences, no. 18, pp. 31-51
- Al-Fares, M., Loukissas, A. and Vahdat. A. (2008) "A scalable, commodity data center network architecture". In SIGCOMM
- Applegate, D. A., Calinescu, G., Johnson, D. S., Karloff, H., Ligett, K. and Wang, J. (2007) "Compressing rectilinear pictures and minimizing access control lists", in Proc. ACM-SIAM SODA, Jan. 2007, pp. 1066–1075.
- Ahmat, K. A. and Elnour, A. (2012) "Towards Effective Integrated Access Control Lists in Internet Networks", The International Conference on Security and Management (SAM), Las Vegas, Nevada
- Abedin, M., Syeda, N., Latifur, K., Bhavani, T.(2006) "Detection and Resolution of Anomalies in Firewall Policy Rules", In Proc. 20th IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec 2006), Springer-Verlag, July 2006, SAP Labs, Sophia Antipolis, France
- Borisov, C.M. (2014). "Pattern Recognition and Matching Learning" August 2015, Publisher: IEEE, John Wiley & Sons, New Jersey, USA. Vol. 4, pg. 31-33.
- Bace, R. and Mell, P. (2009), Special Publication on Intrusion Detection Systems, Infidel Inc and National Institute of Standards and Technology (NIST).
- Bsufka, K., Kroll-Peters, O. and Albayrak, S. (2016) "Intelligent network-based early warning systems," in *Lecture Notes in Computer Science*, Springer, 2016, pp. 103-11.

- Bartal., Y., Mayer, A., Nissim, K. and Wool, A. (1999) “Firmato: A Novel Firewall Management Toolkit”, Proceedings of 1999 IEEE Symposium on Security and Privacy, May 1999.
- Beeky, P., Balachandran, A., Miu, A., Russell, W., Voelker, G. M. and Wang, Y.-M. (2010) PAWNs: Satisfying the Need for Secure Ubiquitous Connectivity and Location Services. *IEEE Wireless Communications Magazine, Special Issue on Future Wireless Applications*, pages 40–48,
- Barman, M.E. and Krankis, G.O. (2016). “Detecting Impersonation Attacks in Future Wireless and Mobile Network” Publisher: IEEE, John Wiley & Sons, New Jersey, USA. Vol. 3, pg. 13-16
- Cliford, S.O. (2015). “Denial of Service Vulnerability in Wireless Devices” Sept. 2015, Publisher: IEEE, John Wiley & Sons, New Jersey, USA. Vol. 2, pg. 7-10.
- Durgin, N. and Mitchell, J.C.S (2015). “A Compositional Logic for Proving Security Properties of Protocol” August 2015, Publisher: Pearson Prentice Hall, 2nd Edition, New Delhi, pg. 90-95.
- Fredrik, B and Dimov, C. (2010). “Wireless Access Points and ARP Poisoning” Jan. 2010, ACM, Publisher: Association for Computing Machinery New York, Vol. 6, pg. 18-21.
- Gobjuka, H. and Ahmat, K. (2011) “Fast and Scalable Method for Resolving Anomalies in Firewall Policies”, in The 14th IEEE Global Internet Symposium (In conjunction with the 31st IEEE International Conference on Computer Communications (INFOCOM 2011), Shanghai, China, 2011.

Authors Profile

Aniekwe, Nkiruka Vivian is a masters candidate at the Department of Electronic and Computer Engineering, Faculty of Engineering, Nnamdi Azikiwe University, Awka, Anambra State. Her research interest is in the area Information Technology, Data transmission and security. She can be contacted via email: viviananiekwe@gmail.com or call +2347032772234.

Ufoaroh Stephen U. is a lecturer at the Department of Electronic and Computer Engineering. His research interest is on Communication and Control Engineering. He is a registered Engineer with Council for regulation of Engineering in Nigeria (COREN) and a professional member of the institute of Electrical and a professional member of the institute of Electrical and Electronics Engineers (IEEE) He can be contacted via sufoaroh@yahoo.com or call +2348035018583.

Alumona, Theophilus is a PHD holder in Electronic and Computer Engineering. He has a Masters degree in Communication engineering from Nnamdi Azikiwe University, Awka, Anambra State, Nigeria. He also holds a B.ENG in Electronic and Computer Engineering. His areas of interest includes: modeling and simulation of communication networks, expert systems, intelligent control, and wireless sensor networks, forensic computing, and many other areas. He is a member of the Nigeria Society of Engineers (NSE), Council for regulation of Engineering in Nigeria (COREN), and IAENG.

1
2