

An Improved Model for Securing Ambient Home Network against Spoofing Attack

Solomon A. Akinboro

Bells University of Technology/ Department of Computer Science and Information Technology, Ota, Nigeria
E-mail: akinboro2002@yahoo.com

Adebayo Omotosho

Landmark University/ Department of Computer Science, Omu-Aran, Nigeria
E-mail: bayotosho@gmail.com

Modupe O. Odusami

Covenant University/ Department of Electrical and Information Engineering, Ota, Nigeria
E-mail: dupfem@yahoo.com

Received: 27 September 2017; Accepted: 07 November 2017; Published: 08 February 2018

Abstract—Mobile Ad hoc Networks (MANET) are prone to malicious attacks and intermediate nodes on the home network may spoof the packets being transmitted before reaching the destination. This study implements an enhanced Steganography Adaptive Neuro-Fuzzy Algorithm (SANFA) technique for securing the ambient home network against spoofing attacks. Hybrid techniques that comprises image steganography, adaptive neuro-fuzzy and transposition cipher were used for the model development. Two variant of the model: SANFA and transpose SANFA were compared using precision and convergence time as performance metrics. The simulation results showed that the transpose SANFA has lower percentage of precision transmitting in a smaller network and a higher percentage of precision transmitting in a larger network. The convergence time result showed that packet transmitted in a smaller network size took longer time to converge while packet transmitted in a larger network size took shorter period to converge.

Index Terms—Spoofing, Steganography, MANET, Home network, Ambient, Transposition cipher, Adaptive-neuro-fuzzy.

I. INTRODUCTION

The volume of wireless communication between mobile users is becoming more popular than ever. The proliferation of mobile computing and communication devices such as cell phones, laptops, handheld digital devices, personal digital assistants and wearable computers is driving a revolutionary change in our information society [1]. The advent of wireless communication between two nodes and the ability of a node to communicate beyond its radio transmission range using intermediate nodes have also led to the growth of Mobile Ad hoc Networks (MANET) [2]. MANET is a connection of two or more devices with wireless

communications and networking capability that communicate with each other without the aid of any centralized administrator [3][4]. Ambient Intelligence (AmI) is the integration of digital devices and networks into the everyday environment, rendering accessible, through easy and natural interactions, a multitude of services and applications. It places the user at the centre of the information society [6]. The objective of AmI is to broaden the interaction between human beings and digital information technology through the use of ubiquitous computing devices. The ubiquitous communication enables digital devices to communicate with each other by means of ad hoc or wireless networking.

MANET nodes are interconnected through wireless interface and the dynamic nature of this type of network makes it highly susceptible to various link attacks. Transmission takes place in an open medium and this makes MANETs highly vulnerable to security attacks [6][7]. The security attacks in MANET can be roughly classified into either active or passive attacks [8]. Actions such as impersonation (masquerading or spoofing), modification, fabrication and replication are active attacks. The security of wireless mobile ad hoc networks is low because MANET has no clear line of defence, it is accessible to both legitimate network users and malicious attackers. This research presents the development of a model capable of preventing spoofing attacks by providing an improved security mechanism that will limit unauthorized user from gaining access to home networks

II. RELATED WORK

In [9] a protocol called Authenticated routing for Ad hoc network (ARAN) which detects and protects against malicious actions by third parties and peers by introducing authentication, message integrity and non-repudiation as a part of a minimal security policy. The result showed that the protocol is simple compared to

most non-secured ad hoc routing protocols. One of the limitations of ARAN is that in networks with heavier data traffic loads, congestion could prevent the discovery of the shortest path. [10] developed a reputation based scheme called a Trustful ARAN which is an integration of ARAN and reputation based scheme. The scheme proves to be more efficient and more secure than Normal ARAN in defending against both malicious and authenticated selfish nodes. The limitation of the approach is that the improvement that was achieved was at a higher cost. [11] developed a solution using network steganography to prevent spoofing attack by the use of a covert channel to transmit messages without any malicious node finding out. The limitation of this approach is that network sniffer can detect the covert channel. [12] presents a mechanism known as Trust Scheme which was developed and this improves the performance of routing protocol against malicious attack by observing nodes behavior. The result shows that the trust scheme improves network efficiency in MANET. The disadvantage of the mechanism is that the observer nodes detected the misbehaving nodes based on the number of received and inaccurate packets. Further research should include observing more factors such as accuracy of the received packets.

In more recent works, [13][14][15] developed a generalized spoofing attack detection which make use of a non-cryptographic mechanism to detect spoofing. The performance was evaluated using detection rate, false positive rate, delay metric, energy level and hit rate. The results showed that the mechanism is more efficient in identifying the attackers than isolating attackers. Also, [16] proposed a novel system called mobile spoofing attack detection and localization in wireless networks (MODELWIN) which uses mobile spoofing attack and localization (MODEL) algorithm. Simulation results revealed that that the model can detect spoofing attacks with a very high detection rate and localize adversaries accurately. One of the limitations of the model is that the original and the attacker node should have different moving patterns. None of the related works, has addressed the problem of spoofing attack in AmI home network, thus the need for this research. We proposed a model with high precision and low convergence time to prevent spoofing attacks in home network using LSB, adaptive neuro-fuzzy and Transposition cipher so that communication will be between legitimate nodes.

III. METHODOLOGY

The proposed model was designed using MANET concept, image steganography, adaptive neuro-fuzzy and transposition cipher. In this approach, the cover images used have their colors represented in decimal as described by binary color combination. The packet sent is then hidden in the least significant bit of the cover image. A transposition cipher was used to rearrange the stegno image before transmission, transposition cipher key was used to decrypt the steganography image while the adaptive neuro-fuzzy was used to train the packets.

A. Copy Conceptual Architecture for the Developed Spoofing Detection in MANET

The developed conceptual model for the Mobile Ad hoc spoofing attack prevention shown in Fig. 1 is a hybrid of two networks MANETs and social networks. The AmI home comprises home server, local devices, remote home devices and MANET. The home control server contains the applications that coordinate the activities of the home. The MANET is the network used to connect all the mobile devices in the AmI home and remote users within the MANET coverage area. The AmI home is connected to the remote users through the internet using the social network platform such as Facebook, Twitter, Myspace or LinkedIn. Through the Social Network Site, the AmI was integrated into the social network.

With the communication route established, the home user's devices are protected from spoof attacks using the enhanced Steganography Adaptive Neuro-fuzzy Steganography Algorithm (SANFA) consisting of least significant bit steganography, transposition cipher and adaptive neuro-fuzzy.

B. Description of the Least Significant bit Algorithm

The least significant bit (LSB) insertion method is a simple steganography algorithm that takes the least significant bit in some bytes of the cover medium and swaps them with a sequence of bytes containing the secret data in order to hide the information in the cover medium. It is a simple approach for embedding message into an image. The LSB technique varies according to the number of bits in an image. Applying LSB technique to each byte of an 8-bit image, only one bit can be encoded into each pixel, as each pixel is represented by one byte. The 8th bit of the cover image is changed to the bit of the secret message. Messages are encoded in different colour components by taking advantage of the fact that the changes in the value of the LSB are imperceptible to human eyes.

C. Description of Transposition Cipher Algorithm

The transposition cipher (or permutation cipher) simply rearranges the values within a block to create the cipher text. This can be done at the bit level or at the byte (character) level. For example, with transposition key pattern : 1 -> 4, 2 -> 8, 3 -> 1, 4 -> 5, 5 -> 7, 6 -> 2, 7 -> 6, 8 -> 3, the cipher key will be 36275184. In this key, the bit or byte (character) in position 1 (with position 1 being at the far right) moves to position 4 (counting from the right), and the bit or byte in position 2 moves to position 8, and so on. The key to the cipher is the pattern of rearrangement.

D. Transposition Cipher Algorithm

- i. Create an empty string variable say P (P is the variable for holding the message) and another variable say H as the holder of the output;
- ii. String P = ""; String H = "";
- iii. Create an empty string variable say K (K is the variable for holding the key)

- iv. String K = “”;
- v. Enter the message in bits; P = “message”;
- vi. Enter the randomly generated key K = “key”;
- vii. Create an array that’s equal to the message
- viii. String [] transposition_cipher = new String [P.length];

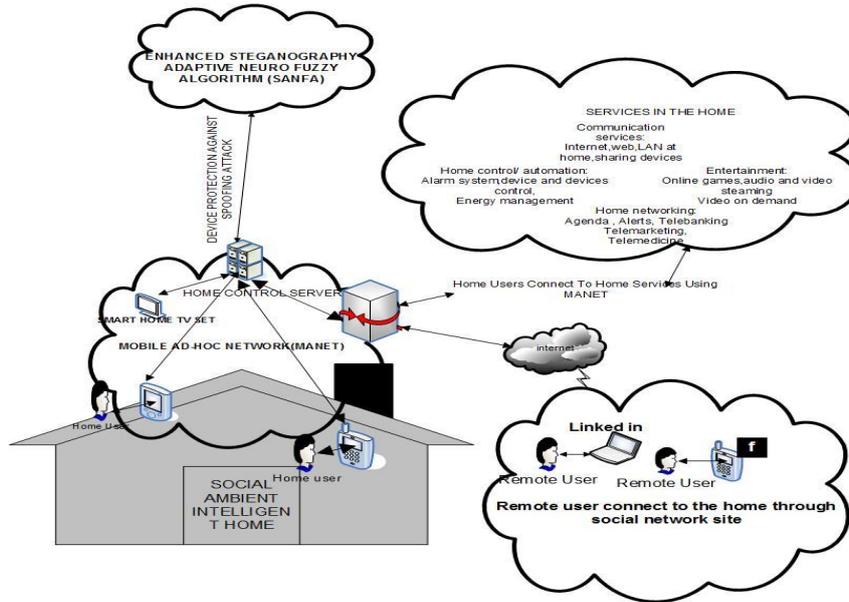


Fig.1. Conceptual Architecture for the Developed Spoofing Detection in MANET

- ix. For (int i = 0; i < P.length; i++)
transposition_cipher[i] = P(i)-1;
 - x. For Int i = 0; i < K.length; i++;
H += transposition_cipher [K(i)-1];
 - xi. Print H;
- normalized weight
- $$w_i = \mu_{A_i}(b_1) * \mu_{B_i}(b_2) * \mu_{C_i}(b_3) * \mu_{D_i}(b_4) * \mu_{E_i}(b_5) * \mu_{F_i}(b_6) * \mu_{G_i}(b_7) * \mu_{H_i}(b_8)$$
- For i = 1 to 8

E. Description of the Adaptive Neuro-Fuzzy System

The adaptive neuro-fuzzy is a system that trains the movement of packets from one node to another in order to avoid the packets being altered by intermediary nodes. The system design is such that the bits of the encrypted message been sent from the key pattern cryptography algorithm will be taken as the input for the adaptive neuro-fuzzy system. The connecting peers, number of peers, membership function and the input from the key pattern cryptography algorithm are all used to get the output image. The membership function is mapped with the input which is the bits of the message to form or get the normalized weights, which is then used to calculate the output of the image.

The output image is compared with the threshold value to make sure the threshold value has been reached so that we can guarantee that the packet has been delivered.

F. Developed Enhanced Steganography Adaptive Neuro-Fuzzy Algorithm (SANFA)

The proposed scheme is a hybrid algorithm which consists of neuro-fuzzy, least significant bit and transposition cipher. The following steps are involved.

- i. Input the bits of the encrypted message been sent from the transposition algorithm
- ii. process the encrypted bit to find the

$$\bar{w} = \frac{W_i}{\sum_{i=1}^s W_i}$$

For i = 1 to 8

- iii. Calculate the output for the image

$$O_i = \frac{\sum_{i=1}^s P_i \bar{W}}{\sum_{i=1}^s \bar{W}}$$

Where

- P = connecting peers
- S = number of connecting peers
- μ = membership function
- b₁ – b₈ = stegno bits or transposed bits (binary packets)
- w = weight of stegno bits or transposed bits

The threshold value must be exceeded before the image can said to be delivered.

G. Performance Evaluation Method for Spoofing Attack Model

In this research work, the proposed enhanced steganography adaptive neuro-fuzzy algorithm is benchmarked against the least significant bit steganography. The parameters used for benchmarking are precision and convergence time.

H. Precision

Precision (P) is computed as the ratio of the number of correctly detected samples to the total number of samples. The P was considered for both the stegno image and the transposed stegno image in Table 1.

The precision for the enhanced steganography adaptive neuro-fuzzy model is computed as follows:

$$P = \frac{Tp}{Tp + TN} * 100$$

Where:

T_P = the number of packets with correct delivery value.
T_N = the number of packets with incorrect delivery value

I. Convergence Time

Convergence time is measured in terms of iterations needed to compute the correct delivery value for the transmitted packets. Convergence time is the number of iteration with respect to the network size. The set threshold value is used as the reference for its computation.

IV. SIMULATION RESULTS AND DISCUSSION

Simulations were performed for the two variants of the proposed enhanced steganography adative neuro-fuzzy for eight (8) encrypted bits in twenty (20) packets to get image output value. The packets was gotten from observing a university wireless campus area network for five days, while the connecting peers were generated using pseudo random numbers generator.. We assumed the threshold value for the simulation to be 0.5. Simulation was done with MATLAB 7.0. The image output were derived by performing at most ten (10) iterations. Table 1 shows the image output value for transmitting one of the twenty (20) packets and Table 2 shows the simulation parameters

Simulation for precision is shown in Table 3 in which

the packets that are transmitted between two and three peers have low percentage precision of 0% and 25% for both SANFA and transpose SANFA respectively, as a result of no intermediary nodes. Also the network with more connecting peers has high percentage precision between 87.5% to 100% for SANFA and 75% to 100% for transpose SANFA. This is an indication that transpose SANFA is a good system for securing ambient home network against spoofing. Result for precision is shown in Table 3. The simulation for the convergence time was performed using twenty scenarios. It takes the average number of iterations for the twenty (20) packets sent and the network size of each packet. The result for the convergence time was shown in Fig. 2, transpose SANFA had 8.875 to 10 secs average for convergence time while SANFA. had 8.75 to 10 secs average for convergence time with small network size. This is so because there is nothing to detect hence the system will not converge faster. For the larger network size, transpose SANFA had 1.875 to 4.75 secs average for convergence time while SANFA had 1.375 to 5.125 secs average for convergence time. The convergence time for transmitting the packets is slightly close for both SANFA and transpose SANFA but when the network size is very high transpose SANFA converges faster than SANFA.

V. CONCLUSION

In order to secure the home network against spoofing attack, a model called enhanced steganography adaptive neuro-fuzzy (SANFA) was developed in this research, in which it comprises of least significant bit steganography, transposition cipher and adaptive neuro-fuzzy. Two variants of the model: SANFA and transpose SANFA were compared using precision and convergence time as performance metrics.

The simulation results showed that SANFA is a good system for securing the home network against spoofing attack. Future work will to secure the home by transmitting message through trusted path depending on how trustworthy are the neighboring nodes.

Table 1. Parameter and Simulation Result of Image Output for Transmitting Fourteenth Packet

Color combination	Message(Packet) 40kbps (replacing the LSB Of the colors)	Transmitted Packet (transposedPacket)	Number of iterations	Output value For stegno image	Number of iterations	Output value For transposed packet
Yellow (11111111, 11111111,0)	11111110 11111110	10111111 10111111	5 8	0.8015 0.5817	3 5	0.7782 0.7404
Green (0,11111111,0)	11111111	11111111	3	0.8818	2	0.6052
Cyan (0,11111111, 11111111)	11111110 11111111	10111111 11111111	7 3	0.6196 0.8170	10 1	0.7297 0.6597
Red (11111111,0,0)	11111110	10111111	6	0.5055	6	0.5003
Blue (0,0, 11111111)	11111110	10111111	8	0.5239	10	2.1471
Red (11111111,0,0)	11111110	10111111	1	0.7926	2	0.9372

Table 2. Simulation Parameters

Transmitted packet(kbp/s)	Binary	Network size
65	01000001	3
132	10000100	16
82	01010010	18
35	00100011	9
146	10010010	5
104	10101100	15
66	01000010	2
93	01011101	14
97	01100001	7
78	01001110	15
64	01000001	11
13	00001101	21
90	01011010	18
40	00101000	24
18	00010010	11
61	00111101	6
42	00101010	3
2	00000010	23
88	01011000	6
44	00101100	12

Table 3. Precision Results for the Transmitted Packets

Packet Size (kbp/s)	Network size	T_p (stegno)	T_p (transposed)	T_N (stegno)	T_N (transposed)	P(%) (SANFA)	P(%) (transpose SANFA.)
65	3	2	0	6	8	25	0
132	16	8	8	0	0	100	100
82	8	8	8	0	0	100	100
35	9	8	8	0	0	100	100
146	5	7	8	1	0	87.5	100
104	15	8	8	0	0	100	100
66	2	0	0	8	8	0	0
93	14	8	8	0	0	100	100
97	7	8	8	0	0	100	100
78	15	8	8	0	0	100	100
64	11	8	8	8	0	100	100
13	21	7	8	8	0	87.5	100
90	18	8	8	8	0	100	100
40	24	8	7	6	1	100	75
18	11	8	8	8	0	100	100
61	6	8	8	7	0	100	100
42	3	0	2	2	6	0	25
2	23	8	7	7	1	100	87.5
88	6	8	8	8	0	100	100
44	12	8	8	8	0	100	100

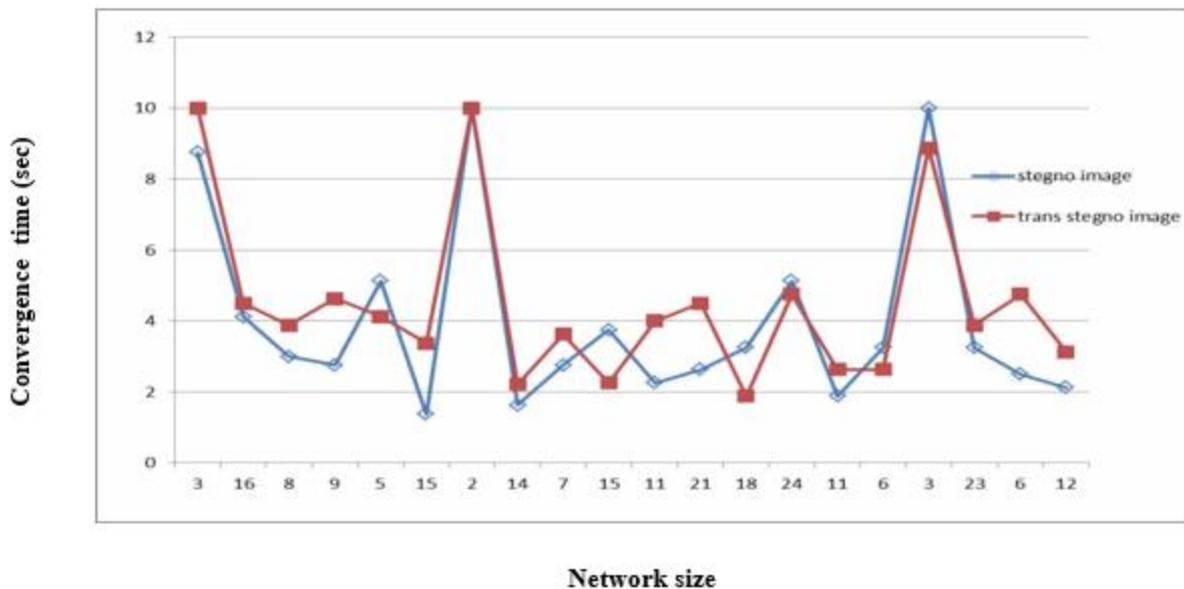


Fig.2. Convergence Time for Transmitting Packets

REFERENCES

- [1] Kumar, Manish, M. Hanumanthappa, and TV Suresh Kumar. "Intrusion Detection Systems Challenges for Wireless Network." *International Journal of Engineering Research and Applications* 2, no 1 (2012): 274-280.
- [2] Misra, Sudip, Isaac Zhang, and Subhas Chandra Misra, eds. *Guide to wireless Ad Hoc networks*. Springer Science & Business Media, 2009.
- [3] Al-Omari, Saleh Ali K., and Putra Sumari. "An overview of mobile ad hoc networks for the existing protocols and applications." *International journal on applications of graph theory in wireless ad hoc networks and sensor networks* 2, no.1 (2010) 87-110.
- [4] Balasubramanian, Venkatraman, and Ahmed Karmouch. "An infrastructure as a Service for Mobile Ad-hoc Cloud." In *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*, pp. 1-7. IEEE, 2017.
- [5] Yang, Hao, Haiyun Luo, Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: challenges and solutions." *IEEE wireless communications* 11, no. 1 (2004): 38-47.
- [6] Kumar, Pawan. "Analysis of different security attacks in MANETs on protocol stack A-review." In *International Journal of Engineering and Technology*, 1, no. 5 (2012): 269-275.
- [7] Saad, Aws, Tareq Rahem Abdalrazak, Ammar Jameel Hussein, and Amer Mohammed Abdullah. "Vehicular Ad Hoc Networks: Growth and Survey for Three Layers." *International Journal of Electrical and Computer Engineering* 7, no. 1 (2017): 271.
- [8] Jawandhiya, Pradip M., Mangesh M. Ghonge, M. S. Ali, and J. S. Deshpande. "A survey of mobile ad hoc network attacks." *International Journal of Engineering Science and Technology* 2, no. 9 (2010): 4063-4071.
- [9] Sanzgiri, Kimaya, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, and Elizabeth M. Belding-Royer. "Authenticated routing for ad hoc networks." *IEEE Journal on selected areas in communications* 23, no. 3 (2005): 598-610.
- [10] Mishra, Mahendra Kumar, Ashish Khare, and Mukesh Dixit. "A Trustful Routing Protocol for Ad-hoc Network." *Global Journal of Computer Science and Technology* 11, no. 8 (2011): 16-26.
- [11] Bhaya, Wesam, and Saud A. Alasadi. "Security against Spoofing Attack in Mobile Ad Hoc Network." *European Journal of Scientific Research* 64, no. 4 (2011): 634-643.
- [12] Yang, Jie, Yingying Chen, Wade Trappe, and Jerry Cheng. "Detection and localization of multiple spoofing attackers in wireless networks." *IEEE Transactions on Parallel and Distributed systems* 24, no. 1 (2013): 44-58.
- [13] Singh, Ankit, Pallav Sinha, and Soumyajyoti Bhattacharya. "Detection and Localization of IDS Based Spoofing Attackers in Wireless Sensor Networks." *International Journal of Computer (IJC)* 27, no. 1 (2017): 103-111.
- [14] Khamayseh, Yaser, Ruba Al-Salah, and Muneer Bani Yassein. "Malicious nodes detection in MANETs: behavioral analysis approach." *Journal of Networks* 7, no. 1 (2012): 116 -125.
- [15] Gracy, Amala, and Chinnappan Jayakumar. "Identifying and locating multiple spoofing attackers using clustering in wireless network." *International Journal of Wireless Communications and Mobile Computing* 1, no. 4 (2013): 82-90.
- [16] Maivizhi, R., and S. Matilda. "Detection and Localization of Multiple Spoofing Attackers for Mobile Wireless Networks." *ICTACT Journal on Communication Technology* 6, no. 2 (2015): 1112 – 1118.

Authors' Profiles



Solomon A. Akinboro is a Senior Lecturer from Bells University of Technology, Ota, Ogun state, Nigeria, holds a B. Tech degree in Computer Engineering from Ladoko Akintola University of Technology, Ogbomosho, M.Sc. and PhD in Computer science from Obafemi Awolowo University

Ile-Ife. Research interests include Distributed system and computer network, Mobile Computing and Machine Learning. Member of the following professional bodies: Nigeria Computer Society, Nigeria Society of Engineers and Council for the Regulation of Engineering in Nigeria



Adebayo Omotosho received his PhD in Computer Science at Ladoko Akintola University of Technology in 2016. He is a Seasoned Computer Programmer and has taken part in a number of programming competitions in C/C++/C#. He is a member of the Nigeria Computer Society (NCS), Computer Professional [Registration Council] of Nigeria (CPN), Computer Science Teachers Association for Computing Machinery (ACM), and International Association of Computer Science and Information Technology. His research interests are health informatics, computer security, machine learning and biometrics.



Modupe Odusami obtained a B.Eng. degree in Electrical Engineering at the University of Ilorin in 2000. She further obtained her Master's degree (M.Sc.) in Information Technology from the Bells University, Ota in 2015. She is currently pursuing her Ph.D. in Computer Engineering at the Covenant University, Ota. She is a member of several professional bodies such as the Nigerian Society of Engineers (NSE), Institute of Electrical and Electronics Engineers (NIEEE), She has published in scholarly journals both National and International. Her current research interests include Software Engineering, Embedded System, Computer Security and Networking. She is a Lecturer II at the Department of Electrical and Information Engineering, College of Engineering, Covenant University, Ota, Ogun State, Nigeria. She is happily married with three kids.

How to cite this paper: Solomon A. Akinboro, Adebayo Omotosho, Modupe O. Odusami, "An Improved Model for Securing Ambient Home Network against Spoofing Attack", *International Journal of Computer Network and Information Security (IJCNIS)*, Vol.10, No.2, pp.20-26, 2018. DOI: 10.5815/ijcnis.2018.02.03