Design and implementation of new security architecture for wireless network

Design and implementation of new security architecture for wireless network

Mohammed M. Mahaba[1, 5], Mohammed H. Megahed[2, 6], Atef Ghalwash[3, 7] and Mohammed Abu Rezka[4, 8]

[1] College of Computing and Information Technology, AASTMT, Cairo, Egypt
[2] Communications Department, Canadian International College (CIC), Cairo, Egypt
[3] College of Computers and Information systems, Helwan University, Cairo, Egypt
[4] College of Computing and Information Technology, AASTMT, Cairo, Egypt

[5] Mohamahaba@gmail.com
[6] mmega080@uottawa.ca
[7] atef_ghalwash@yahoo.com
[8] coe.aastmt@gmail.com

Abstract. Tactical Networks rely on modern communication technologies to connect soldiers and commanders engaged in the battlefield and enable enhanced information flow and data gathering, allowing for decision making based on real-time data analysis. Tactical network is a wireless communication network where wireless tactical network security is a milestone because a soldier does not know from where and when the attacks come.In this paper, a dangerous attack over the deployed tactical network is proposed through group of drones which are sent to the tactical network headquarter. The drone's mission is to identify every device MAC, IP, Name and Location to intercept data or destroy the devices. Also, in this paper, a proposed solution is given for this proposed attack through changing MAC, IP, Name and Location for every device in the headquarter periodically according to the attack time and the devices importance. The MAC, IP, Name and Location must be changed before the drones return to enemy territories.A software program is developed to change MAC, IP, and Name periodically from centered server with no conflicts. The performance analysis for the proposed solution have been taken into consideration the metrics of packets drops, time delay, communication overhead and storage overhead during the changing time. A software tool verifies the changing of IP, MAC and Name for every device. This solution ensures that before the drones return to enemy territories all devices fixed parameters of MAC, IP, and Name are changed.

Keywords: *Tactical Wireless Networks; MAC; IP; Name; Angle of arrival.*

1. INTRODUCTION

Wireless network is a network set up by using radio signal frequency to communicate among computers and other network devices. Sometimes it's also referred to as WPAN, WLAN, WMAN and

WAN [1]. These networks are getting popular nowadays due to easy to setup feature and no cabling involved.

Tactical network security is the prevention of unauthorized access or damage to computers, devices or headquarters that are using the wireless networks [2], [3].

Tactical networks generally contains the application layer, transport layer, network layer [4], medium access control (MAC) layer [5] and physical layer [6]. These protocol layers are typically protected separately at each layer against security threats and vulnerabilities to meet the security requirements, including the authenticity, confidentiality, integrity and availability [7], [8].

In this paper a proposed attack over tactical network is explained and its solution is also given.

One of the most important threats to wireless tactical networks is the theft of information from devices, where the attacker uses drones that are sent within the range of our forces from a distance to steal this information inside headquarter of tactical network and then return back to the starting point to unload such information. These drones can receive signals between devices and by using special antenna they can locate these devices. These drones not only stop locating devices but also gathering packets exchanged between devices to analyze these packets and get devices' information (position, IP, MAC address and name). By using these data the attackers could draw a digital map to the attacked wireless network contains all devices' MAC address, IP and device Name.

These aircraft are launched from a distance from the location of the attacked devices, e.g. the drones' normal speed is 100 km / H and the distance between the headquarter and the enemy is more than 100 km, and these drones are not connected to ground station and have not direct connection with satellite.

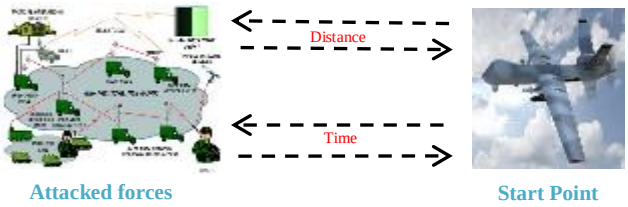

Figure 1. Tactical Wireless Network Threats

The drones need at least 2.30 H to finish the task of entering the headquarter area to steal information and then return back to download its load as shown in figure 1,and the headquarter has drones detector system which detect drones between 1:2 km, an attacker can attack the tactical network as detailed below:

1.1. IP Attacks

1.1.1.IP spoofing attack [9].

IP spoofing is used for generating a forged IP address with the goal of hiding the true identity of the attacker or impersonating another network node for carrying out illicit activities [9]. The network node that receives these packets associated with a forged source IP address will send its responses back to the forged IP address.

1.1.2.IP session hijacking [2].

IP hijacking is another illegitimate activity launched by hijackers for the sake of taking over another legitimate user's IP address [2].

1.2. MAC Address Attacks

1.1.3. MAC flooding [9].
MAC flooding is a technique employed to compromise the security of network switches. Essentially, MAC flooding inundates the network switch with data packets that disrupt the usual sender to recipient flow of data that is common with MAC addresses [9].

1.1.4. MAC spoofing [10], [13].
MAC spoofing is a method in which the alteration in the network interface of a network device is performed on the organization's assigned MAC address [10], [13].

1.3. Name Threat
It is a modern threat in the tactical wireless networks, because the name of the device is often a definition of this device. In the tactical networks, if the attacker knows the name of the device, he will be able to determine the importance of this device, such as headquarters.

1.4. Angel of Arrival Threat (AoA)
AoA measurement is a method for determining the direction and location of pirate radio stations or of any military radio transmitter and devices. [11].

The proposed solutions to counter the proposed attack are:

1) Changing IP, MAC address and name together without any conflict in the network.
2) Changing parameters to each device in time less than drone's trip.
3) Changing each device's information depends on two main major factors: Time period (T) and/or priority. Priority is set according to the device importance. T is set less or greater than 2.30 H as shown in figure 1.

Based on pervious points 1, 2 and 3 the attackers will not be able to attack devices on the network especially after changing device's information or even keep track attacks to the same device because (IP, MAC, Name and location) are changed periodically.

This paper is organized as section 2 introduces related work. Section 3 introduces proposed model. Section 4 introduces proposed model algorithm. Section 5 introduces performance analysis. Section 6 introduces software implementation. Section 7 introduces proposed model testing. Section 8 introduces comparison between new architecture model and previous work. Section 9 introduces conclusion and future work.

The contribution of this paper is as following:

1) Proposed attack: Depends on how the attackers could use drones as shown in figure 1.
2) Proposed attack Solution: Includes how an integrated protection system for a set of devices can be implemented within a single wireless network or a set of connected wireless networks by means of a system that changes the devices' information according to T or priority.
3) Design Hybrid technique: Changing MAC to prevent attacks is an old method used through different tools before but for one PC. New proposed technique depends on the same idea but changing IP, MAC and name at the same time to each PC in same wireless network without any conflict.
4) Software implementation for server and clients: We built new software to achieve the new security architecture model.
5) Performance analysis: Includes packets drops, time delay, time period and priority, setup time and storage overhead.

2. RELATED WORK

In this section, we present a brief overview for related works about wireless network's threats and countermeasures.

Wireless networking has many advantages and many disadvantage [3]. But, it considered a good environment for network threats. Spoofed MAC addresses [10], [13], angel of arrival attack, Man in the middle attack [2] and IP spoofing [9] are just a few of the attacks and threats in wireless network.

S. Jung, J.H. Kim, and S. Kim [12] proposed a modular solution called TMS module to protect and prevent MAC spoofing by using MAC address spoofing attack tools and analyse MAC addresses or sequence numbers through packet dump.

A. Kotkar, A. Nalawade, S. Gawas and A. Patwardhan [9], these researchers pointed to the most important threats affecting the performance and efficiency of wireless network, it also mentioned how to resist such threats. They mentioned MAC flooding and the countermeasure for this kind of threats is port security for wired network and for (Implementations of IEEE 802.1X suites), it often allow packet filtering rules. For Session hijacking they proposed Encryption, String as Session key and Regenerating of Session ID after a Successful Login as countermeasures for such an attack. Encryption and Authentication are countermeasure for IP spoofing.

A. Gupta and R. Kumar Jha [13] illustrated Internet Protocol Security (IPsec) as a method could be used to prevent spoofing attacks. MacChanger, SirMACsAlot, SMAC and wicontrol are tools used for security against MAC spoofing attack. Dsniff and Ettercap-NG are tools can be used to counter Man in the Middle attack.

Y. Zou, J. Zhu, X. Wang, L. Hanzo and Fellow [1] also reported a general classification for wireless network in four types: Physical-Layer Attacks, MAC-Layer Attacks, Network-Layer Attacks and Transport-Layer Attacks. In each type they report the attack name, how it works through the network and its side effect.

N. Hubballi and N. Tripathi [14] introduced the effective of IP address spoofing in the network and how IP address spoofing is commonly used in DDoS attacks. They designed and conducted several scenarios of IP address spoofing in a real network and verified the detection.

Previous studies have shown the most important threats to wireless network and explained how to overcome such threats, but did not mention some other types of threats such as name threat and AoA methodology. Also previous studies mentioned countermeasure to each attacks but did not mention the effects of these countermeasures on satisfying the security requirements [7], [8]. IP attacks and MAC address attacks and how to overcome them have been mentioned, but the impact of tools and methods used to overcome such threats have not been mentioned. It also noted that there is no method or tool can be used to protect wireless network from these both types of attacks.

3. DESIGN OF PROPOSED SECURITY ARCHITECTURE

In next section we illustrate two parts, first part presents design parameters and second part presents software steps which achieves proposed model's goals.

3.1. Design Parameters

The new architecture model that we proposed has some challenges according to the nature of our proposed model as we listed below:

3.1.1. Drones Speed

We proposed a solution to prevent the drones' attacks depending on drones' normal speed and drones' detection system. According to drones' speed we calculated the period time needed to change each device's information in less time than it takes to steal information as shown in figure 1.

3.1.2. Distance between drones' start point and attacked forces.

Distance between the headquarter and the enemy is almost greater than 100 km if the distance is less than 100 km there will be two cases:

1. The period time, network usage overhead and communication overhead will change and increase.

2. According to small distance, ground station could be used to connect directly with the drones to be able to get drones information instantaneous. In this case the proposed solution will not be effective and need some advanced feature to deal with this case.

But if the distance is more than 100 km then the proposed solution and performance will be enough.

3.2. Software Steps

We implemented software to achieve these goals in 5 steps as follows:

3.2.1. Installation

In this step we choose the network security administrator's PC to act as a server and install the software. Then we start to install the software on other PCs to be clients and start connection with the server.

3.2.2. Processing

As shown in figure 2, the server builds the compressed and encrypted message then sends it to each client. When the client receives the new message, first check if NIC not busy then apply the new configuration.

3.2.3. Save and Broadcast

In this step the server saves / updates into the database the acknowledgment message which built and sent by the software (ACK). Then the server builds new message to broadcast for announcing other devices with the new information about the changed device.

3.2.4. Test Period Time and Priority

As shown in figure 3, the server checks the period time and priority to each client to start new iteration of changing IP, MAC and Name to network's devices.

3.2.5. Control All Servers

This steps shows that the chosen devices (administrators' PCs) which are set to be servers they are also controlled with another device (main server) and the same server's software. This is necessary step to control and apply new security architecture model for more than one network.

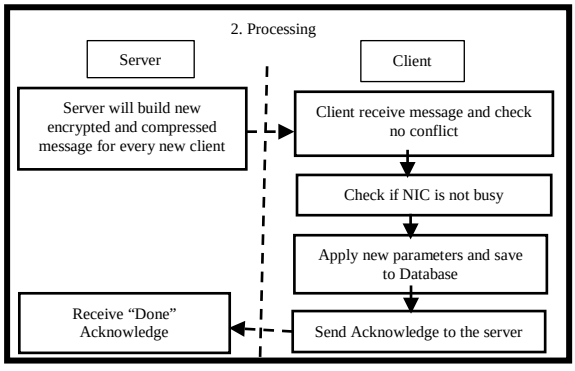

Figure 2. Processing.

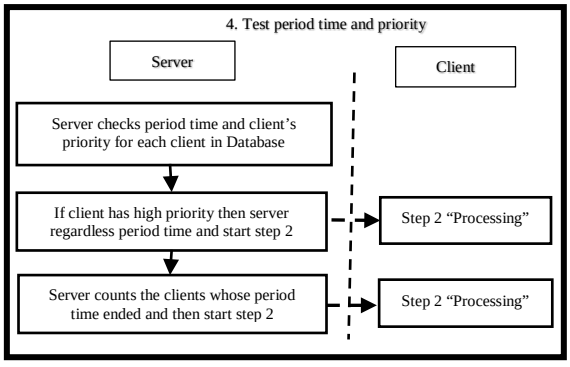

Figure 3. Test Period Time and Priority.

4. PROPOSED MODEL ALGORITHMS

The proposed model is completely based on changing device information every period of time or priority without any conflict with other devices.

We applied this methodology through software by following some steps and applying the next algorithms and dataflow to create, encrypt, compress and build messages to send to network devices.

4.1. Server software algorithm

Algorithm 1. Server Algorithm.

After installing server software	
1: Start connection:	Server initiate UDP connection to listen / send / receive clients' connections.
2: receive new message:	New message from new/old client.
3: check message type:	Each message come from/to clients or server has message type.
4: message type "new user":	Build new message as shown in figure 4 and figure 5 and send it to client.
5: message type "ACK":	Receive ACK from client that new configuration has been applied. If " ACK " from new user then Save parameter and recalculate T from table 2 or set priority. Else update client row in database. Broadcast the ACK parameter to all other clients / servers as shown in figure 3.
6: check priority:	Server check continuously the last time update and priority to each client in database. If time is done Count clients. For count client then Go to step 4 End
7: check T is done:	According to table 2 the server starts changing all network PCs take into consideration equation (1, 2).

In server algorithm we control clients and send messages, also keep IP, MAC and name unique. Algorithm 1 shows the server algorithm.

4.2. Client software algorithm

Algorithm 2. Client Algorithm.

After installing client software.	
1: Start connection:	Clients initiate UDP connection on a specific port to send / receive messages.
2: send message to server:	When clients connect with server they send message to identify themselves.
3: receive message:	Server response with message according to client type new or old user.
4: check:	If message type is new user then Apply new parameters if NIC is not busy or wait until it get free as shown in figure 3.Save new parameter into database
5:check configuration :	New parameters contains new PC name and to be applied OS must be restarted this will not happen until NIC isn't busy. And new IP isn't in use
6: message type "Broadcast":	If message type is Broadcast then Client save/update this message in database which means there is one or more PC has been changed.

In client algorithm network security administrator installs, configures and set priority. Algorithm 2 shows the client algorithm.

4.3. Message structure and dataflow

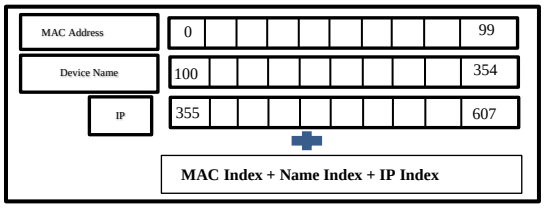

Figure 5. Message structure.

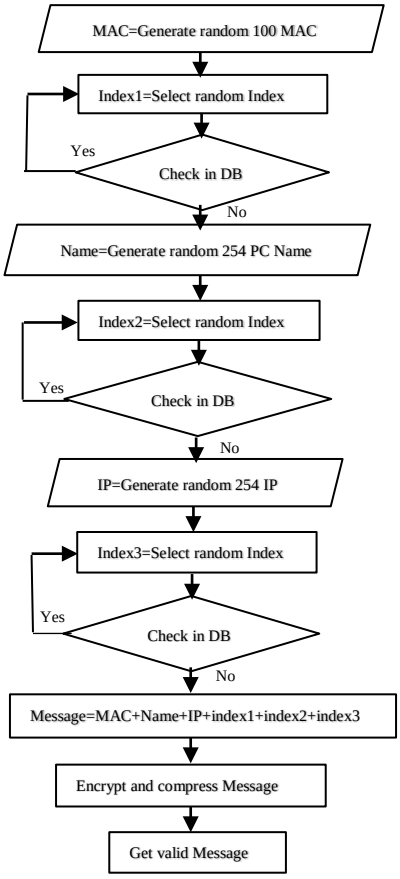

Figure 4. Message dataflow.

In this point we will illustrate the message and how to build this message as shown in figure 5 and figure 4. The message consisting of two parts, first part is a string array of 607 item divided into three parts, part contains 100 MAC address start from 0 to 99, part contains 254 Name start from 100 to 354 and part contains 254 IP address from 355 to 607.

Second part is three numbers each number expresses an index first one for MAC address, second number for device name and third number for IP address. Now we have one message for one client but before we send it, still one more step compress and encrypt the message.

Next section illustrate the dataflow of each part in the message structure.

4.3.1. Generate IP Address dataflow

Generate IP depends on server's IP. First step gets current IP e.g. (192.168.10.45) then we start filling an array contains IPs start from 192.168.10.2 to 192.168.10.254. Second step is choosing random index and check if this is current IP address, if database contains this IP or if there are other device use the same IP. If no then this is a valid index if yes repeats.

4.3.2. Generate MAC Address Dataflow

To create one valid MAC address there are some steps we have to follow in the same sequence. First, generate first byte and make the least two significant bits (10).second, generate second byte by adding first byte to random number. Then we random the reaming four byte. Finally we check if the output

string length is 12, if it does not contains invalid characters (ex :?,",@,#) and if the second byte is equal (2, 6, A or E). If conditions are yes, valid MAC, if no repeats.

4.3.3. Generate Name Dataflow
To create a valid PC's name. First, create a variable "PC_" then we start filling an array contains Names from PC_1 to PC_254. Second step is to choose random Name's index.

5. PERFORMANCE ANALYSIS

The proposed security architecture is characterized by its ability to prevent wireless network threats and attacks and applying new configuration without any conflict. In this section we make the performance analysis through Packets Drops, Time Delay, Time Period and Priority, Storage Overhead, Setup Time and Communication Overhead.

5.1. Packets Drops

Means the numbers of packets which will be lost during applying the device configuration, but according to our proposed solution we will check NIC first if it busy or not to apply this configuration. This means packet drops will not happen except in one case when we enforce the device to apply new configuration because the NIC has been busy for a long period of time, in this case there will be packets lost according to wireless network type and speed as shown in table 1.Also when changing the computer name we must restart the computer and this will give rise to packets drop.

Table 1. Network's Channel Capacity

	Theoretical	Actual
802.11b	11 Mbps	5.5 Mbps
802.11a	54 Mbps	20 Mbps
802.11g	54 Mbps	20 Mbps
802.11n	600 Mbps	100 Mbps
802.11ac	1300 Mbps	200 Mbps

5.2. Time Delay

Means the time which each device needs to apply the new configuration, it is estimated by 10 seconds. Also the time needed to restart the computer after changing name, is different from one device to another according to OS.

5.3. Time Period and Priority

Means the time which is needed to change all PCs' information in the tactical network for one time this called T. We can calculate T from next equation (1).

$$T = (\text{PC No}/\text{No PC Change}) * MT \quad (1)$$

Also T should be equal or less than drones' time as shown in figure 1. But T should meet the condition in equation (2) or network administrator rule for T.

$$T <= 2.5 \text{ hours} \quad (2)$$

Based on, figure 1 and equation (1, 2), all PCs will apply the new security architecture as shown in table 2.

The network security administrator can set a device priority as shown in table 3.

Table 2. PC's No and Time Period

PC No	No of PCs can be changed in the same time	Min time to change one PC/s in the network	Time Period
1-19	1	5 Min	T=1.35 H
20-49	3	7 Min	T=(50 Min – 2 H)
50-99	5	7 Min	T=(1.10 H – 2.20 H)
100-149	5	9 Min	T=(3 H – 4.30 H)
150-200	6	9 Min	T=(3.45 H – 5 H)
201-254	7	9 Min	T=4.30 H – 5.30 H

Table 3. Priority and Time Period

Priority type / Time	Priority			
	0	1	2	3
Priority type	Normal	High	Medium	Low
Time (minute)	T	5	10	15

During applying this new feature, network security administrator should take into his consideration that the PCs which will be chosen to have a priority there is reciprocal PC especially with servers to work instead of the main until the main server apply the new configuration.

Where:

T: Time Period.

PC No: number of all PCs in the network.

MT: Minimum time to change one PC.

Means the time period between the first change to PC's information and the next new change on new PC.

$$3 <= MT <= 9 \text{ Minutes} \quad (3)$$

We assumed this time through equation (3), but it can be change according to the network security administrator.

No PC Change: No of PCs can be changed in the same time.

Means number of PCs which will change their information in the same time together according to T.

5.4. Storage overhead

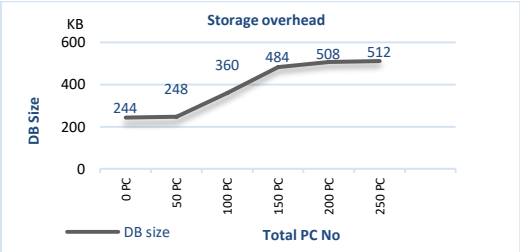

Figure 6. DB File Size.

Means the size which is needed to install our new application and the size which is needed to database file. As shown in figure 6, the changing which happens to database file according to number of PCs in the wireless network. So, storage overhead will not be a problem for applying our methodology.

5.5. Setup time

Means the time we need to install the server software and the client software.

5.6. Communication overhead

Means numbers of packets between server and client/s which will use to change one (device/s)'s information or announce other devices with this new device's information. For announcing there are two ways first multicast and broadcast we will use broadcast because it is easier, save time and less network overhead. Communication overhead in all cases depends on T, No of PCs and PS (Packet Size which almost equal 3.4 KB).

5.6.1. One Network:

i. First PC (client):

$$NU\ (Network\ Usage) = PS \quad (4)$$

PS: Packet Size (the massage which sent from server to the entire client in the same network which equals a row in the database).

ii. Add new PC (client):

$$NU\ (Network\ Usage) = DPS \quad (5)$$

DPS: Database Packet Size (the massage which sent from server to the new client/s which equals all rows in the server database) as shown in figure 6.

$$NU\ (Network\ Usage) = PS * NPC\text{-}1 \quad (6)$$

NPC: number of the connected PCs (all clients) to the server in the network.

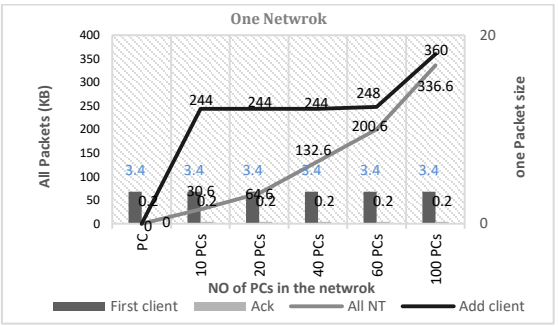

Figure 7. Communications Overhead for One Network

As shown in table 4 and figure 7, we illustrate the total number of packets which will be sent from server to first client or from server to other clients in the same network.

*5.6.2. More than one network:*Means we have some small networks are connecteced toghther with switch/s or router/s .

i. First PC (client):

$$NU\ (Network\ Usage) = PS + (PS*NS) \quad (7)$$

NS: No Of Servers connected with this server.

ii. Add new PC (client)

$$NU\ (Network\ Usage) = DPS \quad (8)$$

$$NU\ (Network\ Usage) = (PS*NPC\text{-}1) + PS*NS \quad (9)$$

Table 4. Packet Size for First Client in More Than One Network

Packet size	first client	Add new client to the network				
		10 PCs	20 PCs	40 PCs	60 PCs	100 PCs
3.4 KB	3.4 KB	30.6 KB	64.6 KB	132.6 KB	200.6 KB	336.6 KB
200 Byte	0.2 KB	0	0	0	0	0

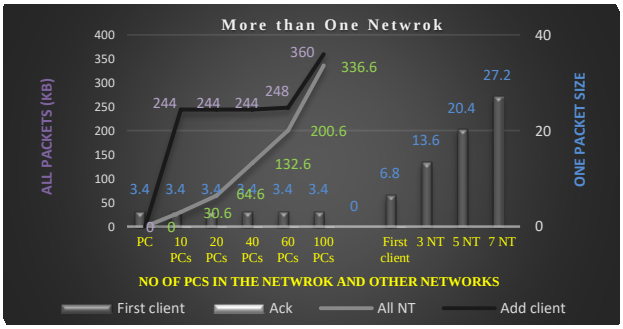

Figure 8. Communications Overhead for More Than One Network.

As shown in table 4, figure 8 and equation (7, 8, 9), we illustrate the total number of packets which will be sent from server to his first client or from server to other servers / clients in other networks.

6. SOFTWARE IMPLEMENTATION

Applying new security architecture model depends on two side as we mentioned above, section 3 and section 4.According to this software which able to achieve our methodology each user will be able to view the database file which contains all information about each device (old IP, old MAC, old Name, new IP, new MAC and new Name), this feature will prevent any disruption can be happened in the network because all user will be updated with the latest information to each device.

6.1. Server software interface: includes selecting NIC and set T time of configuration either manually by network security administrator or automatic which is calculated by software.

6.2. Client software interface: includes selecting NIC and set T time of configuration either priority by network administrator or automatic which is calculated by server software.

7. PROPOSED MODEL TESTING

In order to test the new security architecture model, we will make an experiment in next steps:

First step: downloading a program to monitor the network (e.g. Wireless network monitor) and run this software which is able to detect all devices in the network and get each devices' information.

Second step: applying our new security architecture model to clients.

Third step: run the previous software again which will indicates that the devices information's are changed.

8. COMPARISON BETWEEN NEW SECURITY ARCHETECTURE MODEL AND PREVIOUS WORK

8.1. Threat type and countermeasure

As shown in table 5 symbol (√) means that this attack and its countermeasure is mentioned in that paper.

Table 5. Comparison Between New Security Architecture Model and Previous Work According to Threat Type.

S.No	*Threats type*	S. Jung etal ,[12]	A. Kotkar etal, [9]	A. Gupta etal,[13]	A new security architecture model
1	IP spoofing	X	√	X	√
2	IP hijacking	X	√	X	√
3	MAC spoofing	√	X	√	√
4	MITM	X	X	√	√
5	MAC flooding	X	√	X	√
6	DoS	X	√	√	√
7	AoA threat	X	X	X	√
8	Name threat	X	X	X	√

In this section we made comparison between our methodology in this paper and the other methodologies which are illustrated in other papers and show how the new security architecture model is able to prevent different kinds of network threats at the same time but other methodologies which are illustrated in other papers are able to prevent at most four kinds of network threats.

9. CONCLUSION AND FUTURE WORK

In this paper we introduced a new security architecture model which helps network security administrator to protect and organize his tactical wireless network in new way according to changing (IP, MAC, Name and location).The attackers will not be able to locate or determine which device they are attack or even keep attack to the same device. Also we introduced new algorithms to prevent and protect tactical wireless network from new threats (AoA and name threat). For this new solution we introduced packets drop and communication overhead to avoid packets lost.

Using one time pad encryption algorithm and generate new authentication algorithm between client/s and server are the future work for this new security architecture model. Future work will includes different devices (PC, Mobiles and Tablets) with different OS (android, Windows, Mac OS and Linux).

References

[1] Y. Zou, J. Zhu, X Wang and Lajos H.Fellow,A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends, *proceeding of the IEEE*, 2016.

[2] S R Surya and Dr. G Adiline Magrica, A Survey on Wireless Networks Attacks, *Second Int. Conf. on Computing and Communications Technologies (ICCCT'17)*, pp. 240-247, 2017.

[3] R. U. Rahman and D. S. Tomar, Security Attacks on Wireless Networks and Their Detection Techniques, *Emerging Wireless Communication and Network Technologies*, Springer Nature Singapore Pte Ltd. 2018

[4] R. Jurdak, C. Lopes, and P. Baldi, A survey, classification and comparative analysis of medium access control protocols for ad hoc networks, *IEEE Communications Surveys & Tutorials*, **6**, no. 1, pp. 2-16, April 2004.

[5] M, Takai, J, Martin, and R. Bagrodia, Effects of wireless physical layer modeling in mobile ad hoc networks, *Proceedings of the 2nd ACM International Symposium on Mobile ad Hoc Networking & Computing* (MobiHoc), Carlifonia, USA, September 2001.

[6] C. Saradhi and S. Subramaniam, Physical layer impairment aware routing (PLIAR) in WDM optical networks: Issues and challenges, *IEEE Communications Surveys & Tutorials*, vol. **11**, no. 4, pp. 109-130, December 2009.

[7] C. Kolias, G. Kambourakis, and S. Gritzalis,Attacks and counter- measures on 802.16: Analysis and assessment, *IEEE Communications Surveys & Tutorials*, **15**, no. 1, pp. 487-514, February 2013.

[8] Md. Waliullah and D. Gan, Wireless LAN Security Threats & Vulnerabilities, *Int. J. ACSA*, **5**, No. 1, 2014
[9] A. Kotkar, A. Nalawade, S. Gawas and A. Patwardhan, Network Attacks and Their Countermeasures, *Int. J. of Innovative Research in Computer and Communication Engineering* **1**, Issue 1, March 2013.
[10] M. Dahiya and Dr S. Gill, Protecting MAC Address Spoofing in IEEE 802.11 Using MATLAB, *Int. J. of Advanced Research in Computer Science*, **8**, No. 3, March – April 2017.
[11] M. Schussel, Angel of Arrival Estimation using WiFi and Smartphone, *Int. Conf. on Indoor Positioning and Indoor Navigation (IPIN)*, Alcala de Henares, 4-7 October 2016.
[12] S. Jung, J.H. Kim, and S. Kim,*A Study on MAC Address Spoofing Attack Detection Structure in Wireless Sensor Network Environment*, Department of Multimedia, Hannam University, Daejeon-city, Korea, 2011.
[13] A. Gupta and R. Kumar Jha, Security Threats of Wireless Networks: A Survey, *Int. Conf. on Computing, Communication and Automation (ICCCA2015)*, May 2015.
[14] N. Hubballi and N. Tripathi,An event based technique for detecting spoofed IP packets, *J. ISA*, No. 35, pp. 32–43, 2017.

Appendix

Client algorithm:

Step 1: Connect to the server ()
Step 2: IF first time to connect with the server
Step 3: Send message with message type “new user”
Else
Step 4: Send message with device information and message type “Old user”
End IF
Step 5: While (true)
Step 6: Wait to receive message (Message)
End While
Step 7: decrypt and decompress incoming message
Step 8: IF message type is equal new user or update info
Step 9: IF NIC is not busy
Step 10: apply new parameters
Step 11: save / update new parameters into DB
Step 12: send message to server with message type ACK
Else
Step 13: wait until NIC be not busy, go to step 10
End IF
End IF
Step 14: IF message type is equal broadcast
Step 15: save / update parameters into DB
End IF

Server algorithm:

Step 1: create connection request: Listen ()
Step 2: wait for incoming request: accept ()
Step 3: While (true)
Step 4: Wait to receive message (Message)
End While
Step 5: decrypt and decompress incoming message
Switch (message type)
{

Case new user:
Step 6: Build new message and send it to the new client
Case old user:
Step 7: Update client's row in DB
Case ACK:
Step 8: Update client's row in DB
Step 9: Recalculate T or update priority value in DB
Step 10: Send broadcast message to other clients
}
Step 10: check timer every 5 second
Step 11: IF any client/s it's time up according to T or priority
Step 12: For count client/s
Step 13: Build new message and send to each one
Step 14: Send broadcast message to other clients
End For
End IF