DOI: 10.21917/ijct.2015.0162

DETECTION AND LOCALIZATION OF MULTIPLE SPOOFING ATTACKERS FOR MOBILE WIRELESS NETWORKS

R. Maivizhi[1] and S. Matilda[2]

[1]*Department of Computer Science and Engineering, IFET College of Engineering, India*
E-mail: maivizhi16@gmail.com

[2]*Department of Information Technology, IFET College of Engineering, India*
E-mail: matildags@yahoo.com

Abstract

The openness nature of wireless networks allows adversaries to easily launch variety of spoofing attacks and causes havoc in network performance. Recent approaches used Received Signal Strength (RSS) traces, which only detect spoofing attacks in mobile wireless networks. However, it is not always desirable to use these methods as RSS values fluctuate significantly over time due to distance, noise and interference. In this paper, we discusses a novel approach, Mobile spOofing attack DEtection and Localization in WIireless Networks (MODELWIN) system, which exploits location information about nodes to detect identity-based spoofing attacks in mobile wireless networks. Also, this approach determines the number of attackers who used the same node identity to masquerade as legitimate device. Moreover, multiple adversaries can be localized accurately. By eliminating attackers the proposed system enhances network performance. We have evaluated our technique through simulation using an 802.11 (WiFi) network and an 802.15.4 (Zigbee) networks. The results prove that MODELWIN can detect spoofing attacks with a very high detection rate and localize adversaries accurately.

Keywords:

WLAN Security; Mobile Nodes; Spoofing Attack; Detection; Localization

1. INTRODUCTION

Over the past decades, IEEE 802.11 standard based wireless networks have experienced tremendous growth, becoming an integral part of business, homes and enterprises. The popularity gained is due to many reasons, such as ease of installation, installation flexibility, mobility, reduced cost-of-ownership, and scalability. Providing secure communication is the most important issue in the development of Wireless Local Area Networks (WLANs). Due to the broadcast nature of wireless communication, an adversary can easily hinder the signal or interrupt the normal operation of the network. Although security mechanisms were not designed for early versions of WLANs, nowadays standards and methods are emerging for securing WLANs [1]. Even though various security mechanisms have been developed to secure WLAN, it is still possible for malicious clients to launch variety of attacks.

Spoofing attacks are serious threats that will affect the successful deployment of wireless networks. By passively sniffing the identity of a legitimate device, an attacker can easily launch identity-based spoofing attacks. These attacks significantly impact the normal operation of wireless networks. Further, these attacks facilitate a variety of attacks such as data modification, Denial-of-Service (DoS) attacks, session hijacking and man-in-the-middle attacks [2], [3], [4].

In an 802.11 networks, if management and control frames are not protected, then identity-based spoofing attacks are feasible. The traditional cryptographic schemes will fail if the key is broken and the identity-based spoofing attacks are still possible [5], [6], [7]. Under the above circumstances, there is an increasing interest in using the physical-layer information or characteristics to detect identity-based spoofing attacks in wireless networks [8]–[16]. Recently, researchers used RSS (Received Signal Strength) information, a physical property associated with wireless devices, for detecting and localizing spoofing attacks. However, techniques using RSS will work only for static wireless networks. For mobile environments, these RSS profiles changes with respect to node mobility. Consequently, they raise excessive false alarms in mobile wireless networks. The damage will be serious if these attacks are carried on mobile wireless devices. As wireless networks are integrated with our daily social lives, there is an increasing need to support emerging mobile wireless applications. Although mobility is naturally endowed with wireless networks, little work has addressed identity-based spoofing attacks in mobile scenarios.

In this work, we propose a novel system called mobile spoofing attack detection and localization in wireless networks (MODELWIN) which uses mobile spoofing attack detection and localization (MODEL) algorithm to detect and localize spoofing attacks in mobile wireless environments, which has not been addressed in the previous work. Also, our system determines the number of attackers present in the network. For detection and localization of spoofing attacks, MODEL algorithm uses the distance information between nodes. As mobility is important in wireless network, the key idea of MODELWIN is to use the previous location (prevloc) and current location (currloc) of nodes for detecting spoofing attacks. Even if there is only very little distance between the genuine node and the attacker node, MODELWIN achieves excellent localization performance. Once adversaries are exactly localized, our system eliminates attackers from mobile wireless networks and increases network performance.

The rest of the paper is organized as follows. Section 2 begins with a discussion of recent related research work. In section 3, we provide the MODELWIN framework in detail. Section 4 describes the proposed algorithm. In section 5, we provide the simulation results and in section 6, network performance. In section 7, we conclude our work.

2. RELATED WORK

Cryptographic-based authentication is the traditional approach for preventing spoofing attacks in wireless networks [5], [6], [7]. However, the application of cryptographic schemes requires

reliable key distribution, management and maintenance mechanisms. Cryptographic mechanisms are not always desirable as the authentication key can be compromised. Also these methods incur computational, infrastructural, and management overhead. Further, these methods are not suitable as wireless devices have limited resources and incur significant human management costs.

In recent years, many active researches exploits physical layer characteristics for detecting identity based spoofing attacks in wireless networks. Yang, Chen, Trappe and Cheng [16] proposed the use of Received Signal Strength (RSS), a physical property closely correlated to location in physical space for detecting spoofing attacks, finding the number of attackers and localize multiple adversaries. However, this approach is not always appropriate as the RSS values fluctuate significantly over time due to distance, noise and interference. Also localization is not accurate if the distance between the client and the attacker is very small.

In our previous work [17], we proposed Distance based Detection and Localization (DDL) algorithm which uses distance between two nodes as the basis for spoofing detection, determining the number of attacks, localizing multiple adversaries and eliminates them. However, the above approaches can only work when the wireless network consists of static nodes.

The works [18] and [19] are most closely related to us. Yang, Chen and Trappe [18] partitions the RSS trace of a node identity into two classes, and detect the mobile spoofing attack when the two classes have low correlation. However, it cannot work if the distance between the client and attacker is very small. Also, it takes long time to detect the spoofing attacks with desirable performance.

Zeng, Kannan, Wu and Prasant [19] proposed RCVI (Reciprocal Channel Variation-based Identification) that takes the advantage of the location decorrelation, randomness and reciprocity of the wireless fading channel [20] to detect identity-based spoofing attacks in mobile scenario. Though, this approach works even if the distance between the client and the attacker is small, it suffers from several drawbacks: (a) it requires the sender to send the RSS information, which is an overhead. (b) if the attacking intensity is higher, it is harder to detect the attacks. (c) when the frame interval becomes larger, performance of RCVI degrades. However the above approaches are unable to find the number of attacks present in the network and localize adversaries in mobile wireless networks.

This work differs from our previous study in that we use previous location of nodes in addition to current location and distance information. Furthermore, our work is novel because none of the existing work can detect the spoofing attack, determines the number of attacks, localizes adversaries and eliminates them in mobile wireless environments.

3. MODELWIN

In this section, we discussed our MODELWIN system in detail. Our proposed approach detects the spoofing attack and localizes adversaries for each mobile node identity. Fig.1 shows the MODELWIN system. The system exploits location information for nodes having same identity as input. The proposed system detects the presence of mobile spoofing attacks, determine the number of attacks, localize mobile spoofing adversaries and eliminate the attackers from the mobile wireless network. For performing mobile spoofing detection and localization, MODELWIN uses location table (loctable) and attacker table (atktable).

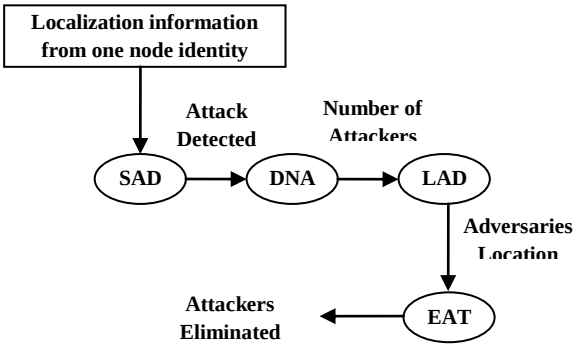

Fig.1. MODELWIN System

The main idea of MODELWIN is to use the prevloc and the currloc of nodes in the network. By customizing the packet format this information can be accommodated in it.

3.1 PACKET HEADER

This paper is simulated using simulation tool. To achieve very high accuracy in detection and localization of mobile spoofing attacks, the structure of the packet is customized to store the location information about the nodes. Generally, a packet consists of packet header and data payload. Packet header stores attributes for packet delivery, while data payload contains user information [21]. We customize the packet header in order to store the physical location of nodes for effective detection and localization of mobile spoofing attacks. Fig.2 shows the customized packet structure.

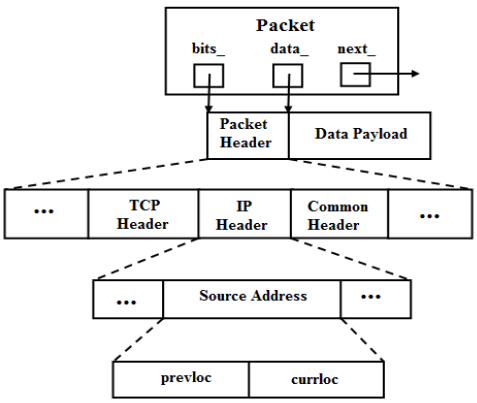

Fig.2. Packet Structure

Here, the source address field is bifurcated into prevloc and currloc. The fields prevloc and currloc corresponds to the physical location of the mobile devices. The field prevloc stores the previous location of the current packet and currloc stores the current location of the current packet. This location information is stored in latitude and longitude (lat-lon) format, in order to accurately localize multiple adversaries. By customizing the packet format, MODELWIN uses the prevloc and currloc of node to find the accurate position of mobile nodes. We designed the 802.11 wireless networks in such a way that the prevloc and

currloc will be automatically embedded in the packet whenever a node is deployed.

3.2 DESIGN OF loctable AND atktable

Fig.3 shows the format of both loctable and atktable.

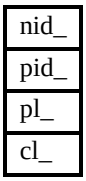

Fig.3. Structure of loctable and atktable

nid_ represents node identity, pid_ represents packet identity, pl_ represents the previous location of the current node and cl_ represents the current location of the current node.For each packet received by the destination with same identity, information about the packets is stored in the loctable to enable spoofing detection and location. We assume that the attack is an active attack and for each transmission the first packet that arrives at the destination comes from the original source. Information about the first packet is stored in the loctable. The movement of the original node is maintained in the loctable. If any attacker interfere the transmission, information about it is stored in a separate atktable. The proposed system maintains a separate atktable for each attacker and stores the attacker mobility it.

3.3 MODULES

MODELWIN consists of the following modules:

3.3.1 Spoofing Attack Detection (SAD):

In this module, MODELWIN takes packets collected from the same node identity as input. Also, we assume that the attack is an active attack. Therefore, during transmission the first packet arrives at the destination always comes from the original source node. Thus for the first packet, prevloc and currloc are stored in the pl and cl fields of the loctable respectively. The destination accepts the first packet. For the remaining packets, MODELWIN has 2 cases.

In the first case, it compares the prevloc with pl of last packet stored in the loctable. If both are same, it compares the currloc with cl of loctable. If this also same, this implies that the source is not moving and transmits packets from the same location and there is no spoofing attack. Otherwise the system declares the presence of mobile spoofing attack.

In the second case, prevloc and pl are different. If so, it compares the cl and prevloc. If both are same, this implies that the source is moved to a different location and there is no spoofing attack. Also the values of pl and cl are updated with prevloc and currloc respectively. Otherwise, the system declares the presence of spoofing attacks.

3.3.2 Determining the Number of Attacks (DNA):

Once SAD declares the presence of spoofing attack, DNA checks the spoofing condition with all existing atktable. If an atktable satisfies the spoofing condition, pl and cl of the respective atktable is updated with the prevloc and currloc. If none of the atktable satisfies the condition for spoofing, a new atktable is created and prevloc and currloc values are stored in it. The number of atktable created for the each transmission will be the number of attackers present in the network.

3.3.3 Localizing multiple ADversaries (LAD):

Once SAD detects the spoofing attack, LAD extracts the prevloc and currloc from the packet and sent to the server along with attacker number for localization.

3.3.4 Eliminating ATtackers (EAT):

Once the spoofing attack is detected, MODELWIN eliminates adversaries from the mobile wireless networks by rejecting packets from the attackers.

4. ALGORITHM

The most challenging task in mobile wireless networks is the development of an effective localized algorithm. These algorithms are a special kind of distributed algorithms where only a subset of nodes in the WLANs participates in communication, and computation. We developed a generic localized algorithm MODEL, for solving spoofing attack problems in mobile wireless local area networks.

Algorithm: MODEL

Input: Packets from same node identity

Output: Detection of spoofing attacks with accurate position of attackers

i=0

loctable=null

get the prevloc, currloc of first packet

loctable(pl)=prevloc

loctable(cl)=currloc

accept the packet

for each of the remaining packet **do**

get the prevloc, currloc

if loctable(pl)==prevloc **then**

if loctable(cl)==currloc **then**

“no attack”

accept the packet

else

“attack”

reject the packet

call ATN(i, prevloc, currloc)

endif

else

if loctable(cl)==prevloc **then**

“no attack”

accept the packet

loctable(pl)==prevloc

loctable(cl)==currloc

else

“attack”

reject the packet

call ATN(i, prevloc, currloc)
endif
endif
endfor

The following pseudo code ATtacker Number (ATN) is used to find the number of attackers present in the network. For each attacker, a separate atktable is created.

Algorithm ATN
Input: Attacker packet
Output: Attacker number
new=true
for j=1 to i **do**
if $atktable_j$(pl)==prevloc **then**
if $atktable_j$(cl)==currloc **then**
new=false
break
else
if $atktable_j$(cl)==prevloc **then**
$atktable_j$(pl)=prevloc
$atktable_j$(cl)=currloc
new=false
break
endif
endif
endfor
send(j)
while new **do**
i=i+1
$atktable_i$(pl)=prevloc
$atktable_i$(cl)=currloc
send(i)
endwhile

The above pseudo codes perform packet level localization robustly. Since we assume an active spoofing attack, any time adversaries may inter/fere the transmission to ruffle the normal operation of the network. So packet level localization is performed by MODEL to accurately localize multiple adversaries.

5. SIMULATION RESULTS

In this section, we evaluate the effectiveness of MODELWIN through simulation for mobile spoofing detection and localization. This paper is simulated in Network Simulator version 2. We simulated MODELWIN using an 802.11 (WiFi) and 802.15.4 (Zigbee) wireless network and introduced different parties: a source node, a destination node and two or more attackers. Any/All these parties can be mobile.

5.1 SPOOFING DETECTION RATE

The Fig.4 presents the mobile spoofing detection rate (both Existing and MODELWIN) versus the distance between the spoofing node and the original node.

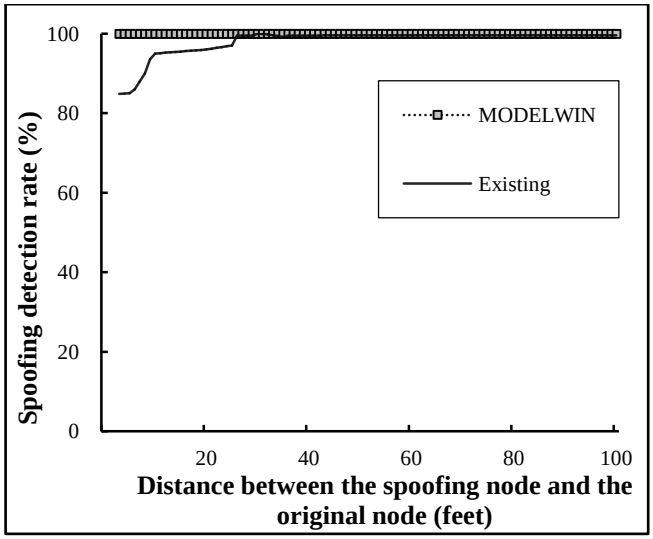

Fig.4. Spoofing Detection Rate

For the existing system, the above graph shows how the attack detector detects a spoofing device in physical space when it is at various distances from the genuine node. It is found that the further away spoofing node is from original node, the higher the detection rate becomes. When the spoofing node is 15 feet apart from the original node, the spoofing detection rate goes to over 90 percent. But the spoofing nodes have the high probability of generating similar RSS traces when they are less than 15 feet away. Hence the detection rate is less than 90 percent, but above 70 percent. However, the likelihood of exposing the attacker himself increases when spoofing node moves closer to original node. When the spoofing node is about 45-50 feet apart from the original node the detection rate goes to 100 percent.

For MODELWIN, the above graph shows whatever the distance between the spoofing node and original node is; the mobile spoofing detection rate will always be 100%.

The Fig.5 shows that, the performance of the existing approaches degrades in detecting the mobile spoofing attacks when the attacking intensity increases. If the attacking intensity is 1, then the number of packets coming from the attacker and source are equal. In this case, the detection rate is about 97%. If the attacking intensity is 2, the detection rate decreases to 85%. This means that performance decreases when attacking intensity increases.

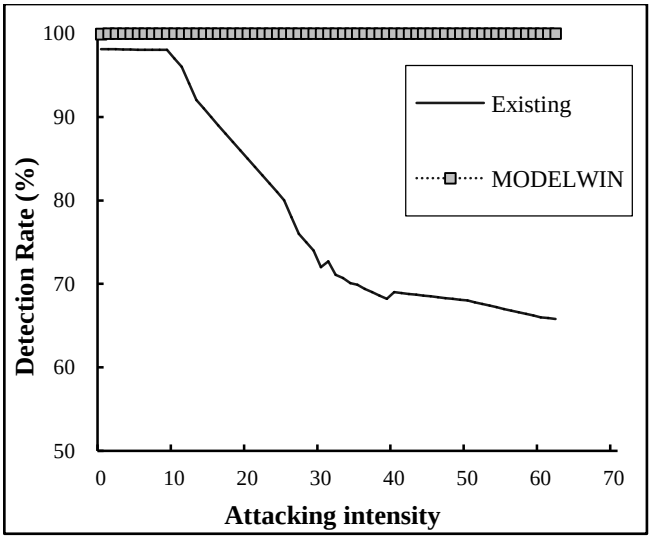

Fig.5. Impact of attacking intensities

In MODELWIN, the rate of spoofing attack detection is always 100% even when the attacking intensity increases.

5.1.1 Comparison of MODELWIN with other approaches

Since the RSS measurements fluctuate significantly over time due to distance, noise and interference, the existing approaches are not always desirable to detect spoofing attacks in mobile wireless networks. Fig.6 shows the comparison of MODELWIN with the existing approaches.

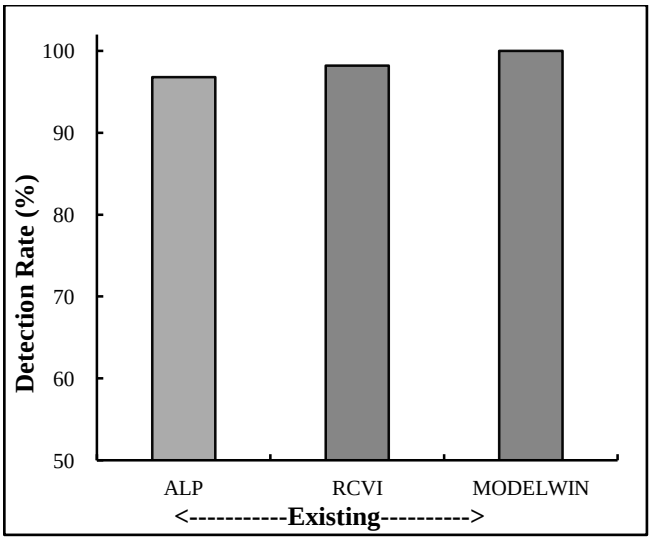

Fig.6. Comparing MODELWIN with existing approaches

It shows that MODEL algorithm detected 100% spoofing attacks and outperformed the existing approaches. As the RSS values are not always accurate, Yang's alignment prediction (ALP) algorithm detected more than 96% attacks and Zeng's reciprocal channel variation-based identification (RCVI) technique detected more than 98% attacks.

5.2 DETERMINING THE NUMBER OF ATTACKS

MODELWIN achieves 100% in number of attacker determination irrespective of whether the attacker node is static or mobile. Our system uses a separate atktable for each attacker to record their moving pattern and thus the number of atktable created determines the correct number of attackers for each transmission in the network.

5.3 LOCALIZING ADVERSARIES

The Fig.7 shows the localization performance of MODELWIN system.

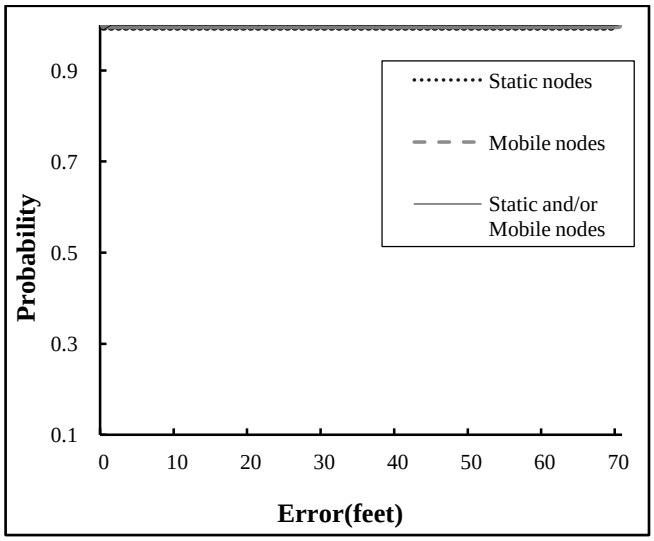

Fig.7. Localization performance

The above graph presents the localization error CDF (Cumulative Distributive Function) for MODELWIN. It shows that MODELWIN algorithm performed well even if the distance between the client and the attackers are very small. MODELWIN works well for wireless networks consisting of static nodes or mobile nodes or static and/or mobile nodes and achieves 100% accuracy in all the cases. Thus our approach will accurately localize multiple adversaries.

6. NETWORK PERFORMANCE

The Fig.8 and Fig.9 shows the effectiveness of using MODELWIN algorithm for detecting the presence of mobile spoofing attacks, determining the number of attacks, localizing multiple adversaries and eliminating all the attackers from the network.

In MODELWIN, the performance of the network can be measured on the basis of packets accepted by the destination. The following figure shows the transmission that takes place at the original source. It shows all packets sent by the original node are received by the destination with few packets dropped. The graph reveals only few packets are dropped by the destination. The key observation from Fig.8 is that almost all packets with same node identities sent by the original node are accepted by the destination.

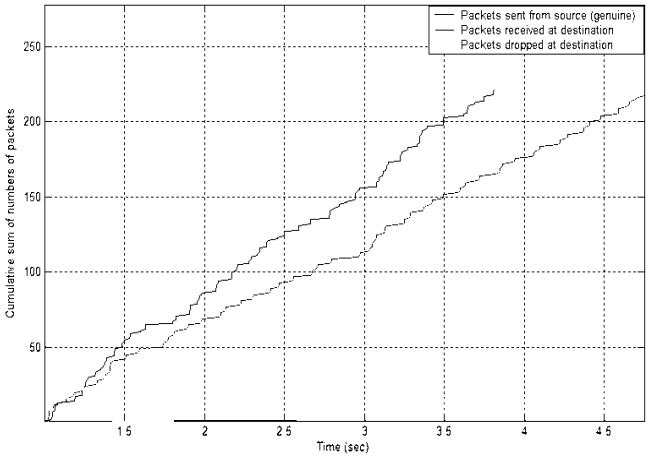

Fig.8. Result of Source (Original) Transmission

The Fig.9 shows the transmission that takes place at the attacker node. It shows all packets sent by the attacker node are received and dropped by the destination. MODELWIN algorithm performs packet-level localization, so that even if a single packet comes from the attacker, MODELWIN algorithm rejects it; thereby it eliminates all attackers from the network and enhances network performance.

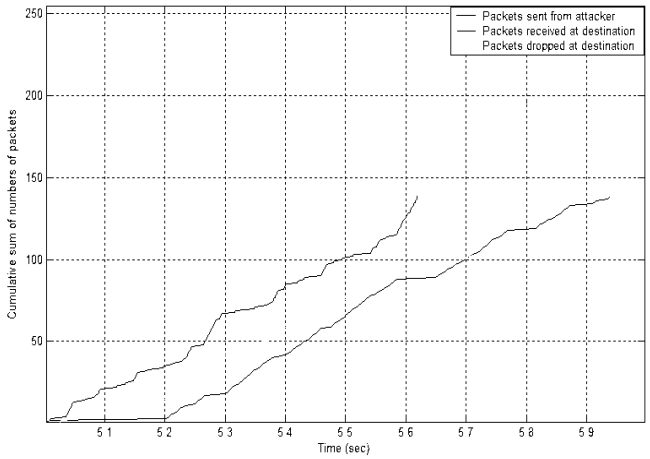

Fig.9. Result of Attacker Transmission

The Fig.8 and Fig.9 reveals that MODELWIN system accepts only packets coming from the original node. It will not accept even a single packet from attackers. This implies that MODELWIN enhances network performance by dropping all packets coming from attackers.

7. CONCLUSION

In this work, we proposed MODELWIN, an approach to detect and localize identity-based spoofing attacks in mobile wireless environments. This problem is not addressed in our previous work. Our proposed technique exploits the previous and current location of nodes to detect the spoofing attacks. Also, it determines the number of attackers present in the network. Simulation results revealed that our work accurately localize multiple adversaries even if the distance between the attacker and the victim node is very small. Additionally, our proposed method eliminates attackers from mobile wireless network and thereby enhances network performance. The only requirement of MODELWIN is that the original and attacker node should have different moving patterns. This implies that nodes should not transmit packets at positions where other nodes (either original or attacker) transmit packets most recently.

REFERENCES

[1] Mohammad O. Pervaiz, Mihaela Cardei and Jie Wu, "*Security in Wireless Local Area Networks*", in "Security in distributed and networking systems", Yang Xiao and Yi Pan,(Eds.), NJ: World Scientific, 2007.

[2] John Bellardo and Stefan Savage, "802.11 Denial-of-service attacks: real vulnerabilities and practical solutions", *Proceedings of the 12th conference on USENIX Security Symposium*, Vol. 12, pp. 15-28, 2003.

[3] F. Ferreri, M. Bernaschi and L. Valcamonici, "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks", *IEEE Wireless Communications and Networking Conference*, Vol. 1, pp. 634-638, 2004.

[4] Martin Eian, "Fragility of the robust security network: 802.11 denial of service", *Applied Cryptography and Network Security: Lecture Notes in Computer Science*, Vol. 5536, pp. 400–416, 2009.

[5] Bing Wu, Jie Wu, E.B. Fernandez and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks", *Proceedings of IEEE International Symposium on Parallel and Distributed Processing*, 2005.

[6] Avishai Wool, "Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation", *Wireless Networks*, Vol. 11, No. 6, pp. 677-686, 2005.

[7] Mathias Bohge and Wade Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks", *Proceedings of the 2nd ACM workshop on Wireless security*, pp. 79-87, 2003.

[8] M. Demirbas and Youngwhan Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks", *International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pp. 564–570, 2006.

[9] Daniel B. Faria and David R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints", *Proceedings of WiSe'06: ACM Workshop on Wireless Security*, pp. 43–52, 2006.

[10] Liang Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the physical layer for wireless authentication", *IEEE International Conference on Communications*, pp. 4646–4651, 2007.

[11] Liang Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A Physical- Layer Technique to Enhance Authentication for Mobile Terminals", *IEEE International Conference on Communications*, pp. 1520–1524, 2008.

[12] Liang Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "MIMO assisted channel-based authentication in wireless networks" *42nd Annual Conference on Information Sciences and Systems*, pp. 642–646, 2008.

[13] Yong Sheng, K. Tan Guanling Chen, D. Kotz and A. Campbell, A, "Detecting 802.11 MAC Layer Spoofing

Using Received Signal Strength", *IEEE 27th Conference on Computer Communications,* pp. 1768–1776, 2008.

[14] Liang Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels", *IEEE Transactions on Wireless Communications*, Vol. 7, No. 7, pp. 2571–2579, 2008.

[15] Vladimir Brik, Suman Banerjee, Marco Gruteser and Sangho Oh, "Wireless device identification with radiometric signatures", *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pp. 116–127, 2008.

[16] Jie Yang, Yingying Chen, W. Trappe and J. Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 24, No. 1, pp. 44-58, 2013.

[17] R. Maivizhi and S. Matilda. "Distance based Detection and Localization of multiple spoofing attackers for wireless networks", *International Conference on Computation of Power, Energy, Information and Communication*, pp. 63-67. 2014.

[18] Jie Yang, Yingying Chen and W.Trappe, "Detecting spoofing attacks in mobile wireless environments," in *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, pp. 1-9, 2009.

[19] Zeng, Kai, Kannan Govindan, Daniel Wu, and Prasant Mohapatra. "Identity-based attack detection in mobile wireless networks", *IEEE Proceedings INFOCOM*, pp. 1880-1888, 2011

[20] Theodore S. Rappaport, "*Wireless Communications: Principles and Practice*", Prentice Hall, 2002.

[21] Teerawat Issariyakul and Ekram Hossain, "*Introduction to Network Simulator NS2*", Springer, 2009.