ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

A Novel Wireless Network By Enforcing Location Distinction Protection Along With Attack Identification

Neenu Lekshmy .S[1], Shiney M Abraham[2]
M.Tech Student[1], Assistant professor[2]
Department of Electronics and Communication Engineering, A P J Abdul Kalam Technological university
[1]neenunandhakumar@gmail.com

***Abstract*— Location distinction is a location based authentication mechanism, which also detect location changes of wireless users. The differences in wireless channel characteristics are used to distinguish locations or identify location changes. A vulnerability of existing location Distinction scheme has been identified by introducing a new attack, called virtual multipath attack. To defend against this attack we propose a detection technique that utilizes an auxiliary receiver or an antenna to identify these fake channel characteristics, we also integrate source authentication in the scheme. These modifications improve secrecy and scalability of the scheme**

Key words: Channel impulse response, Multipath, Security, Source authentication.

I. INTRODUCTION

In wireless networks location distinction is a location based authentication mechanism and also used to detect wireless users location change.To achieve location distinction by using the spatial uncorrelation property of wireless channels specifically, difference in wireless channel characteristics. Recent studies discovered that wireless channel characteristics become uncorrelated every half carrier wavelength over distance (spatial uncorrelation property).

Here, a vulnerability of location Distinction scheme has been identified by introducing a new attack, called virtual Multipath attack. By launching such an attack adversary can easily hide the location changes or impersonate movements by injecting fake wireless channel characteristics into the receiver. The idea of the discovered attack is to create a virtual multipath channel as undetectable to make the receiver.

The proposed detection technique is utilized to detect this attack, which consist of an auxiliary receiver or antenna at multiple locations to identify the virtual multipath channels and characteristics.

Source authentication is also added in the scheme, one of the main challenges of securing multipath communication is source authentication. A major concern of source authentication is allowing a receiver to ensure that the received data is authentic (i.e., It originate from the source and was not modified on the way).

For the source authentication, sender/receiver attacks a MAC to each packet computed by using a key K known only itself. The receiver buffers the received packets without being able to authenticate it. If the packet is received too late then it is discarded. After a short while, sender discloses K and the receiver is able to authenticate the packet.

To demonstrate the success of defence approach, sketch out some of the points

1. Virtual multipath channel created by the attacker can be identified.
2. Create a defence technique to detect such attacks and protect location distinction system.
3. The source authentication scheme provide immediate authentication.
4. Harden the sender &receiver against virtual multipath attack.

II. PRELIMINARIES

A. Creation of virtual multipath

To create virtual multipath channel, first knows the multipath effect which is the reason for the spatial uncorrelation property. Normally wireless signal propagate in the air through multiple paths due to obstacle reflection, diffraction and scattering. Therefore, receiver can observe different channel characteristics from these signal .To fool the receiver; the attacker needs to create a "virtual channel" that can exhibit a multipath propagation similar to real multipath.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

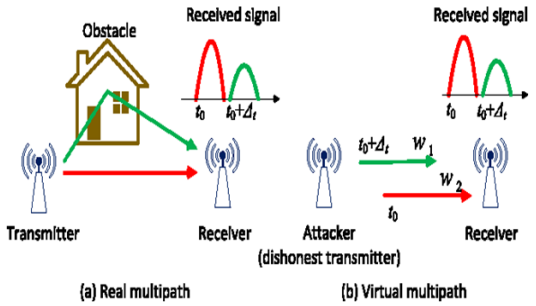


Fig. 1 creating a virtual Multipath

Fig.1. shows a simple multipath scenario ,where signal from transmitter travels on two path one is the reflection path and other is the direct path . At the time t0 receiver receiving signal from direct path and at the time t0 + Δt,the receiver receiving signal copy from the direct path and one from reflection path.

In virtual multipath scenario,there is only one direct path exist between the attacker and receiver.The attacker wants to make the receiver believe that two path exist similar to real multipath, so attacker sends the signal alone first.After Δt attacker superimpose a new signal copy onto the one in transmission.The attacker scale both the signal by a attenuation factor w1&w2 to copy the signal amplitude caused by the realpath.

B. *Channel impulse response*

Due to multipath propagation receiver recevives multiple copies of the signal from different path each of which has a different delay due to the path it traverses .The received signal is the sum of these time delayed copies. Each path imposes a response to the signal and the superposition of all responses between two node is called channel impulse response .

To determine channel impulse response if the transmitter has changed it's location ,the receiver estimate the channel impulse response of received signal and compare it with the previous estimation result .The location change is detected if the difference between the newly estimated impulse responses and the previous one exceeds certain threshold .

C. *Estimating channel impulse response*

Channel impulse responses are normally estimated using the training sequences .The transmitter sends a training sequence over the wireless channels ,while the receiver uses same sequence and the corresponding received signal to estimate the channel impulse response .

Mathematical Formulation:

Channel impulse response calculate using the training sequence and corresponding received samples .Firstly the transmitter converts the training sequences into M physical layer symbols ,then this M symbol send through the wireless channel . Let X denote the transmitted symbols and L denote the paths . Thus, the receiver can receive L copies of X the vector Y of a received symbols the convolution sum of the L copies of X.

x = [x1,x2,...,xM], transmitted symbols

h = [h1,h2,...,hL]T, channel impulse response

y = h∗x + n, received symbols (1)

Where n is the noise ,x is the convolution operator

$$\mathbf{y} = \begin{bmatrix} x_1 & 0 & \cdot & 0 \\ x_2 & x_1 & \cdot & \cdot \\ \cdot & x_2 & \cdot & 0 \\ \cdot & \cdot & \cdot & x_1 \\ x_M & \cdot & \cdot & x_2 \\ 0 & x_M & \cdot & \cdot \\ \cdot & 0 & \cdot & \cdot \\ 0 & 0 & \cdot & x_M \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \\ \cdot \\ \cdot \\ h_L \end{bmatrix} + \mathbf{n} \quad (2)$$

(2) => Y = Xh+n (3)

LS and LMMSE are used to estimate the equation (3)

III . PREVIOUS WORKS

Attack against all existing location distinction approaches that are built on the spatial uncorrelation property of wireless channels. In such an attack, the adversary can easily hide her location changes or impersonate movements by injecting fake wireless channel characteristics into a target receiver. To defend against this attack, a detection technique is used that utilizes an auxiliary receiver or antenna to identify these fake channel characteristics.

This system has lack of accuracy in the attack scenario and the detection of attack is more complex in some cases for example when the attacker is static/dynamic

IV. PROPOSED SYSTEM

A. *Virtual multipath attack*

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

The attacker can launch two types of attacks. In a basic attack, the attacker can use any weights to craft a virtual multipath signal. This will fool the receiver to obtain random, incorrect estimates of the channel impulse response. In an advanced attack, with the knowledge of the real channel impulse response between attacker and the receiver, the attacker is able to compute exact weights that make the receiver estimate the chosen channel impulse responses specified by the attacker.

According to equation 2, the channel estimator models each path by delaying it for one symbol duration. Specifically, the i-th arrived signal copy arrives at time t0 +(i−1)·1/R, where t0 is the arrival time of the first arrived signal copy and R is the transmission symbol rate. Thus, the attacker can superimpose a copy into the transmitting signal at time t'0, t'0+ 1/R, ⋯,t'0 + (L−1)·1/R to emulate L paths, where t'0 is the start time of the attacker's first transmission. Accordingly, the time delay for a signal copy is Δt = 1/R.

B. Sender Setup

A sender distributes a stream of data composed of message chunks $\{M_i\}$. Generally, the sender sends each message chunk M_i in one network packet P_i. Here the receiver can authenticate each message chunk Mi separately.

The sender splits the time into even intervals I_i. We denote the duration of each time interval with T_{int}, and the starting time of the interval I_i is T_i. Trivially, we have $T_i = T_0 + i * Tint$. In each interval, the sender may send zero or multiple packets. Before sending the first message, the sender determines the sending duration (possibly infinite), the interval duration, and the number N keys of the key chain. The sender picks the last key K_N of the key chain randomly and pre-computes the entire key chain using a pseudo-random function F, which is by definition a one-way function. Each element of the chain is defined as $K_i = F(K_i+1)$. Each key can be derived from KN as $K_i = F^{N-i}(K_N)$, where $F^j(k) = F^{j-1}(F(k))$ and $F^0(k) = k$. Each key of the key chain corresponds to one interval, i.e., K_j is active in interval I_j. .

Since we do not want to use the same key multiple times in different cryptographic operations, we use a second pseudo-random function F' to derive the key which is used to compute the MAC of messages in each interval. Hence, $K'_i = F''(K_i)$. Figure 2 depicts this key derivation. We propose to use HMAC in conjunction with a cryptographically secure hash function for the pseudo-random function. A possibility is to use the following: F (x) = HMAC(x,0) and
F '(x) = HMAC(x; 1), where 0 and 1 are 8-bit integers

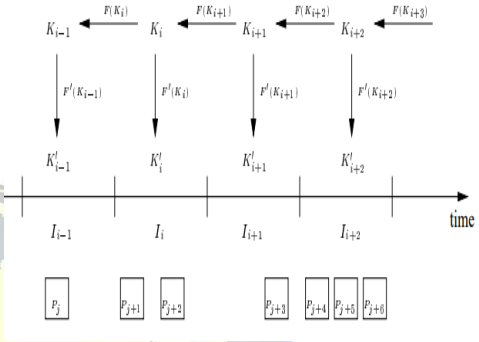


Fig.2. key chain and the derived MAC

D. Receiver Tasks

The receiver must verify for each packet that the key, which is used to compute the MAC of that packet, is not yet disclosed by the sender, and then no attacker could have altered it in transit.

When the receiver receives packet P_j sent in interval I_i at local time t_c, it computes an upper bound on the sender's clock t_j. To evaluate the security condition, the receiver computes the highest interval x the sender could possibly be in, which is $x = [(t_j - T0)/T_{int}]$. The receiver now verifies that $x<I_i + d$ (where I_i is the interval index), which means that the sender must not have been in the interval in which the key K_i is disclosed, hence no attacker can possibly know that key and spoof the message contents.

The receiver cannot, however, verify the authenticity of the message yet. Instead, it stores the triplet (I_i, Mj, MAC (K_i, M_j)) to verify the authenticity later when it knows K'_i. Two possibilities exist on how to handle the unauthenticated message chunk M_j. The first possibility is to hand M_j to the application, and notifies it through a callback mechanism as soon as M_j is verified. The second possibility is to buffer M_j until the authenticity can be checked and pass it to the application as soon as M_j is authenticated.

D. Defense against virtual multipath attack

The intuition behind the defense strategy is that nobody can craft one key to open two different doors. In other words, if a receiver cannot tell

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

whether there is an attack or not, maybe a second receiver can. As a result, this approach uses an auxiliary receiver or antenna, which we refer to as a helper. The helper is placed more than half a wavelength away from the receiver to ensure a distinct channel characteristic. We let the receiver use two different training sequences x1 and x2 to estimate the channel impulse response alternatively.

At the receiver, the virtual channel created by a attacker can result in the same estimated channel impulse responses (equal to the one chosen by the attacker). However, at the helper, the virtual channel leads to different estimated channel impulse responses.

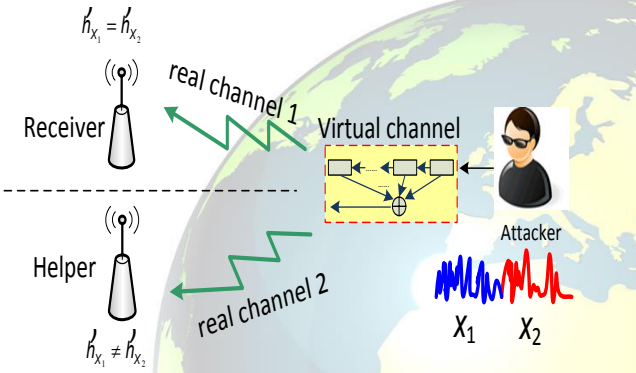


Fig.3 Defense against virtual multipath attacks

E. Defense Analysis

For the first transmission, the attacker must solve the weights, so that the equation $h*x_{a1} = h_a*x1$, x_{a1} is the aggregated signal with weighted time-delayed copies of the training sequence x1. Let h_{help} denote the real channel impulse response between the attacker and the helper corresponding signal received at the helper is $h_{help1}*x1 = h_{help} *x_{a1}$

$$h_{help1} = (X1^{H}X1)^{-1} X1^{H}(h_{help} *x_{a1})$$

For the second transmission, both the receiver and the helper use the training sequence x2 to estimate the channel and the corresponding aggregated signal x_{a2} makes the equation $h*x_{a2} = h_a *x2$, $h^{help2} = (X2^{H}X2)^{-1}X2^{H}(h^{help}*x^{a2})$.

Note that for both transmissions, the channel impulse response estimated by the receiver are always the same, because the weights are "customized" so that the receiver will obtain the attacker's chosen channel impulse response after the channel estimation. X1 ≠ X2. This means the attacker cannot fool the receiver and the helper at the same time.

F .Evaluation of defense method

Here examine how the channel estimation results of the receiver and the helper differ from each other, so that such an inconsistency can reveal the existence of the virtual multipath attack. The helper and the receiver estimate the channel impulse responses from two successive transmissions, and then calculate the Euclidean distance between both estimates. Let d_{helper} and d_{rec} denote the distances computed by the helper and the receiver. We can see that the virtual multipath attack leads to a much larger distance at the helper than the receiver, i.e., $d_{helper} >> d_{rec}$. Specifically, $d_{rec} = 0.0093$ and $d_{helper} = 0.1199$.

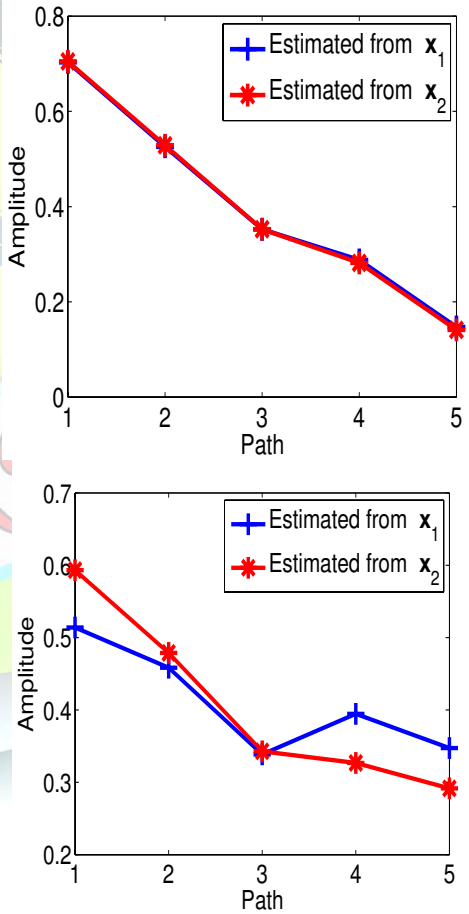


Fig.*4.Recevier and receiver with helper*

G. Simulation result

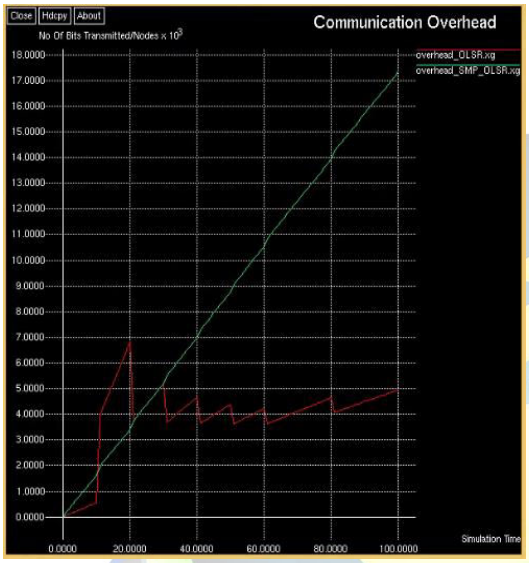
- Low computation overhead. On the order of one MAC function computation per packet for both sender and receiver.
- Low communication overhead. Required is as little as one MAC value per packet.

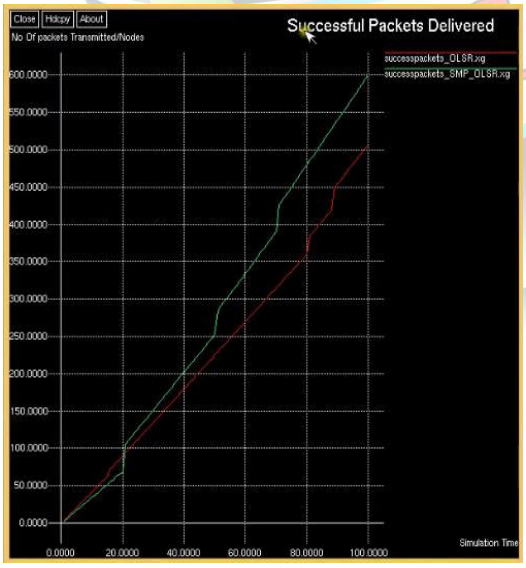
ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

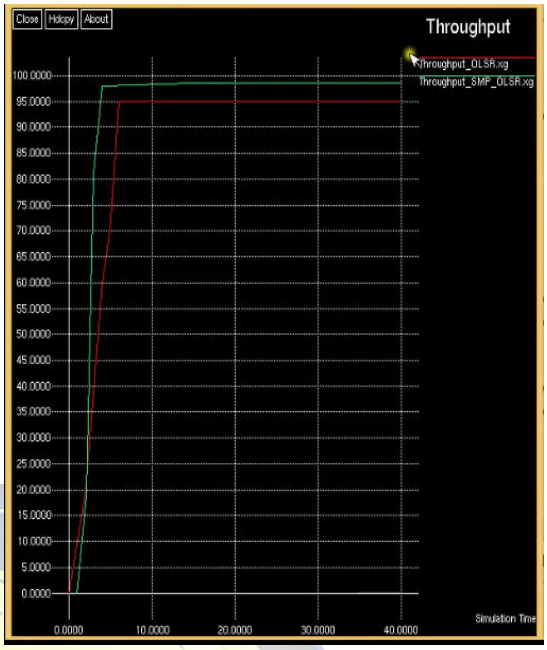
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Periodically, the sender also needs to send out the secret keys.

- Perfect loss robustness. If a packet arrives in time, the receiver can verify its authenticity eventually (as long as it receives later packets).
- Improve scalability of the scheme
- Reduce space overhead for multiple instances
- Detection is possible at any condition.







V. CONCLUSION

In this paper, we presented an extension for existing location distinction approaches. We discover a new attack against all the existing location distinction method built on the spatial uncorrelation property of wireless channels. To defend against this attack, we propose a detection technique that utilizes an auxiliary receiver or antenna to identify these fake channel characteristics .Both source authentication and detection improve the scalability of the method. Reduce the space overhead for multiple instances, increase the resistance to virtual multipath attack.

REFERENCES

[1] Song Fang, Yao Liu, Wenbo Shen, Haojin Zhu and Tao Wang, "Virtual Multipath Attack and defence for location Distinction in wireless networks" In2016 IEEE Transactions on Mobile Computing,2016

[2] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in Proc. of IEEE S&P '10, May 2010, pp. 286–301

[3] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in Proc. of ACM MobiCom '07, September 2007, pp. 111–122.

[4] Y. Liu and P. Ning, "Poster: Mimicry attacks against wireless link signature," in Proc. of ACM CCS'11, 2011.

ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

[5] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" in Proc. of IEEE INFOCOM '13, April 2013

[6] J. Xiong and K. Jamieson, "Secure array: Improving wifi security with fine-grained physical-layer information," in Proc. of ACM MobiCom '13, 2013, pp. 441–452.

[7] A. Perrig, R. Canetti, J.Tygart, and D. X. Song. Efficient authentication and signing of multicast streams over lossy channels. In IEEE Symposium on Security and Privacy, May 2000.]

[8] N. Bhaskar and I. Kouvelas. Source-specific protocol independent multicast. Internet Draft, Internet Engineering Task Force, Mar. 2000. Work in progress.

[9] B. Briscoe. Flames: Fast, Loss-Tolerant Authentication of Multicast Streams. Technical report, BT Research, 2000.http://www.labs.bt.com/people/briscorj/papers.html

[10]] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction," in Proceedings of the Fourth European Workshop on System Security, 2011.

[11] A. F. Molisch, Wireless Communications, 2nd Edition. Wiley India Pvt. Limited, 2007