INTEGRATED CRYPTOGRAPHIC AND WIRELESS LINK SIGNATURES DEPENDABLE FOR WIRELESS SECURITY

M.Krishnamurthy [1], Dr.N.Pughazendi [2], N.Avinash [3] , R.P.Balaji [4], M.Kanagaraj [5]
Department of Computer Science Engineering, Panimalar Engineering College
Chennai, India-600123

ABSTRACT

- Wireless link signature may be a physical layer authentication mechanism, victimisation the multipath impact between a transmitter and a receiver to produce authentication of wireless signals. This paper identifies a brand new attack, known as mimicry attack,against the present wireless link signature schemes. associate degree assaulter can forge a legitimate transmitter's link signature as long because it knows the legitimate signal at the receiver's location, and the attacker doesn't have to be compelled to be at precisely the same location as the legitimate transmitter. we tend to conjointly extend the mimicry attack to multiple-input multiple-output (MIMO) systems, and conclude that the mimicry attack is possible only if the quantity of attacker' antennas is up to or larger than that of the receiver's antennas. To defend against the mimicry attack, this paper proposes a unique construction for wireless link signature, called time-synched link signature, by integration cryptographical protection and time issue into wireless physical layer options. Experimental results make sure that the mimicry attack may be a real threat and therefore the freshly planned time-synched link signatures area unit effective in physical layer authentication.

- **<u>KEY WORDS</u>:** Wireless Link signature, Time - Synchronization, MIMO

- .

INTRODUCTION

- There are multiple proposals in recent years to supply increased wireless security exploitation physical layer characteristics, as well as process wireless devices, authenticating and distinguishing wireless channels, and explanation secret keys from wireless channel options solely evident to the human activity parties. we tend toadditionally extend the mimicry attack to the link signature theme. Since the last link signature theme is basicallyAN integration of the techniques, all existing link signature schemes area unit prone to the mimicry attack. moreover, we discover that if the receiver has 2 antennas to hand in glove certify the transmitter, the assaulter with only 1 antenna cannot with success launch the mimicry attack. However, we tend to discover that the mimic attack continues to be possible if the assaulter additionally has 2 antennas. Then we tend to explore the practicableness of the mimicry attack into MIMO systems. If the amount of the receiver's receive antennas is larger than that of the attacker's transmit antennas, the receiver will sight the mimicry attack, otherwise, the receiver is fooled that the attacker's link signatures area unit identical with those of the documented transmitter's. The mimicry attack will apply to the subsequent example situations once link signatures area unit used for authentication:

- launching location spoofing attacks: AN assaulter will utilize a faux location to fool a target receiver by making a faux wireless link signature;
- bypassing motion detection systems: AN assaulter may maintain its wireless signature unchanged whereas it's really moving, so from the angle of the target receiver, WHO utilizes the wireless link signature to work out whether or not the transmitter moves or not, the assaulter seems to stay stationary;
- bypassing wireless transmitter authentication systems: AN assaulter will impersonate a legitimate transmitter by shaping its wireless link signature

SURVEY

- In 2006 D. B. Faria and D. R. Cheriton,Wireless networks square measure liable to several identity-based attacksin which a malicious device uses solid waterproof addresses to masquerade as a specifc consumer or to make multiple illegitimate identities.For example, many link-layer services in IEEE 802.11 networks are shown to be liable to such attacks even when 802.11i/1X and alternative security mechanisms square measure deployed. In this paper we have a tendency to show that a sending device is robustly identifed by its signalprint, a tuple of signal strength values rumored by access points acting as sensors. We show that, differentfrom waterproof addresses or different packet contents, attackers don'thave the maximum amount management concerning the signalprints they manufacture. Moreover, exploitation measurements in a very testbed network, we have a tendency to demonstrate that signalprints ar powerfully related to with the physical location of purchasers, with similar values found largely in shut proximity. By tagging suspicious packets with their corresponding signalprints, the network is ready to robustly establish every transmitter independently of packet contents, permitting detection of alarge category of identity-based attacks with high chance.

- In 2007 N. Patwari and S. K. KaseraThe ability of a receiver to see once a transmitterhas modified location is vital for energy conservationin wireless detector networks, for physical security of radio-tagged objects, and for wireless network security in detec-tion of replication attacks. during this paper, we tend to propose us-ing a measured temporal link signature to unambiguously determine the link between a transmitter and a receiver. When the transmitter changes location, or if associate degree aggressor at a different location assumes the identity of the transmitter, the pro-posed link distinction algorithmic program dependably detects the modification in the physical channel. This detection is performed at one receiver or collaboratively by multiple receivers. We record over nine,000 link signatures at different locations and over time to demonstrate that our technique significantly increases the detection rate and reduces the warning rate, in comparison to existing strategies.

- In 2008, V. Brik, S. Banerjee, M. Gruteser, and S. Oh,We design, implement, and measure a method to spot the supply network interface card (NIC) of associate degree IEEE 802.11frame through passive radio-frequency analysis. This tech-nique, referred to as PARADIS, leverages minute imperfections oftransmitter hardware that ar noninheritable at manufacture andare gift even in otherwise identical NICs. These imper-fections ar transmitter-specifc and manifest themselves asartifacts of the emitted signals. In PARADIS, we measurediferentiating artifacts of individual wireless frames within themodulation domain, apply appropriate machine-learning classi-fcation tools to attain signifcantly higher degrees of NICidentifcation accuracy than previous best notable schemes.

- In 2010 A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, Ensemble could be a system that uses a set of sure personal devices to supply proximity-based authentication in pervasive environments. Users square measure ready to firmly try their personal devices with antecedently unknown devices by merely inserting them near one another (e.g., users will try their phones by simply delivery them into proximity). Ensemble leverages a user’s growing assortment of sure devices, like phones, music players, computers and private sensors to watch transmissions created by pairing devices.Lower/physical layer characteristics have been considered as potential alternatives/complements to provide security services in wireless networks. This article provides an overview about various non-cryptographic mechanisms for user authentication and device identification in wireless networks using lower/physical layer properties or information. We discuss merits and demerits of these authentication/identification schemes and the practical implementation issues. Future research on crosslayer security design concludes this paper.

- In 2011 K. Zeng, K. Govindan, and P. MohapatraLower/physical layer characteristics are thought-about as potential alternatives/complements to produce security services in wireless networks. this text provides an summary regarding numerous non-cryptographic mechanisms for user authentication and device identification in wireless networks exploitation lower/physical layer properties or info. we have a tendency to discuss deserves and demerits of those authentication/identification schemes and also the sensible implementation problems. Future analysis on crosslayer security style concludes this paper.

- In 2013 H. Liu, Y. Wang, J. Yang, and Y. ChenRecently, there has been nice interest in physical layer security techniques that exploit the randomness of wireless channels for firmly extracting science keys. many attention-grabbing approaches are developed and incontestable for his or her practicability. The progressive, however, still has a lot of space for up their utility. this is often as a result of i) the key bit generation rate supported by most existing approaches is incredibly low that significantly limits their sensible usage given the intermittent property in mobile environments; ii) existing approaches suffer from the quantifiability and flexibility problems, i.e., they can not be directly extended to support efficient cluster key generation and don't suit for static environments. With these observations in mind, we tend to gift a replacement secret key generation approach that utilizes the uniformly distributed section data of channel responses to extract shared science keys beneath narrowband multipath weakening models.The projected approach enjoys a high key bit generation rate as a result of its efficient introduction of multiple irregular section data among one coherence amount because the keying sources. The projected approach additionally provides measurability and flexibility as a result of it depends solely on the transmission of periodical extensions of unmodulated curving beacons, that permits effective accumulation of channel phases across multiple nodes. The projected theme is completely evaluated through each analytical and simulation studies. Compared to existing work that concentrate on pairwise key generation, our approach is extremely climbable and might improve the analytical key bit generation rate by a handful of orders of magnitude.

EXISTING SYSTEM:

- Existing techniques using non-cryptographic approaches to authenticate wireless transmitters can be classified intothree categories: software fingerprinting, location distinction, and radiometric identification. The RSS based methods directly estimate the location of a signal origin using the RSS values. However, such methods can be defeated with an array antenna, which can fake arbitrary source locations. The link signature based approaches authenticate the channel characteristics between the transmitter and the receiver. In radiometric identification approaches, the distinctive physical layer characteristics exhibited by wireless devices are utilized to distinguish between them.

DISADVANTAGES:

- The receiver will not have the same link signature.
- The attacker with only one antenna cannot successfully launch the mimicry attack

PROPOSED SYSTEM:

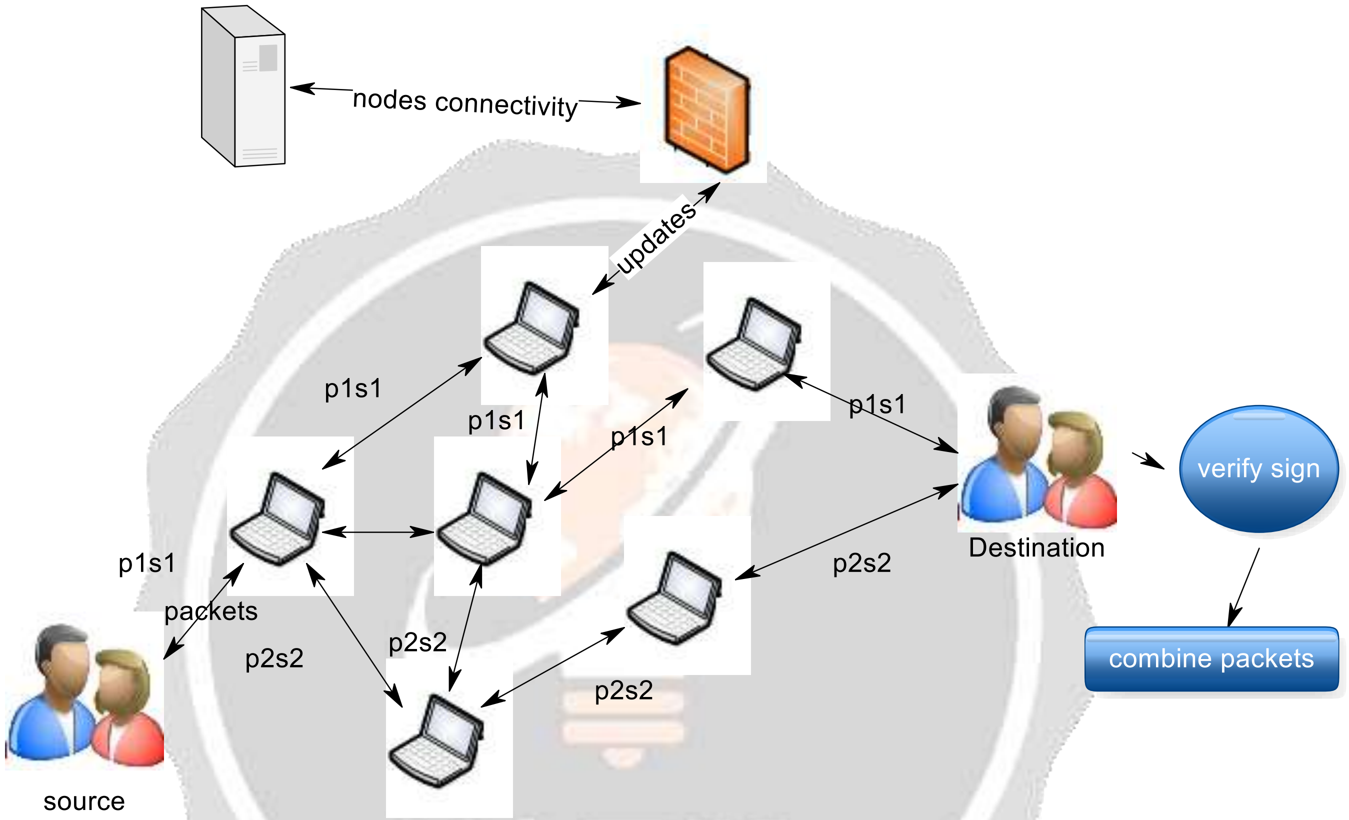
- We identify themimicry attack against these link signature schemes. Then we explore the feasibility of the mimicry attack into MIMO systems. If the number of the receiver's receive antennas is larger than that of the attacker's transmit antennas, the receiver can detect the mimicry attack, otherwise, the receiver can be fooled that the attacker's link signatures are the same with the ones of the authenticated transmitter's. a novel construction for link signature, which is called time synched (i.e., time synchronized) link signature. Time-synched link signature integrates cryptographic protection as well as time factor into the wireless physical layer features, and provides an effective and practical solution for authenticating physical layer wireless signals.Finally, we perform extensive experiments to confirm the threats of the mimicry attack and demonstrate the effectiveness of the time-synched link signature for physical layer authentication.

ADVANTAGES:

- Feasibility of mimicry attacks and the effectiveness of time-synched link signature.

- Attacker utilizing at least the same number of antennas as the receiver's antennas can successfully launch the mimicry attack

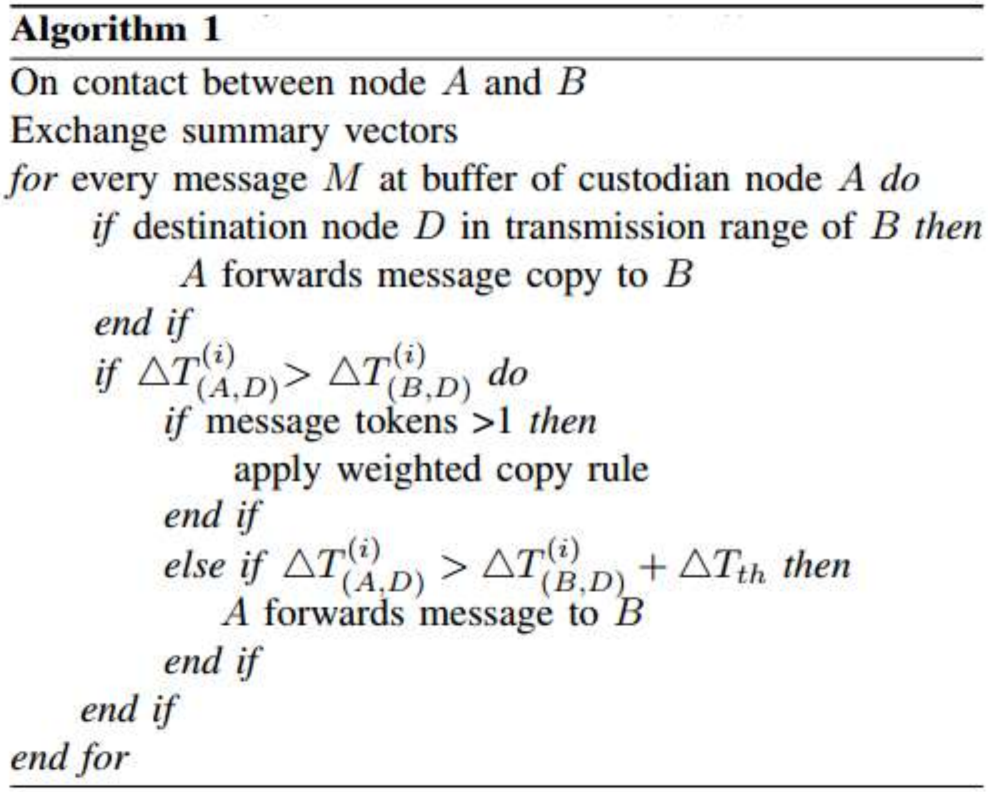
SYSTEM ARCHITECTURE:



AES ALGORITHM:

- AES (acronym of Advanced Encryption Standard) is a symmetric encryption algorithm. AES was designed to be efficient in both hardware and software, and supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. AES mainly used for secure message sharing.

ROUTING PROTOCOL:



Algorithm 1

```
On contact between node $A$ and $B$
Exchange summary vectors
for every message $M$ at buffer of custodian node $A$ do
    if destination node $D$ in transmission range of $B$ then
        $A$ forwards message copy to $B$
    end if
    if $\triangle T^{(i)}_{(A,D)} > \triangle T^{(i)}_{(B,D)}$ do
        if message tokens >1 then
            apply weighted copy rule
        end if
    else if $\triangle T^{(i)}_{(A,D)} > \triangle T^{(i)}_{(B,D)} + \triangle T_{th}$ then
        $A$ forwards message to $B$
    end if
  end if
end for
```

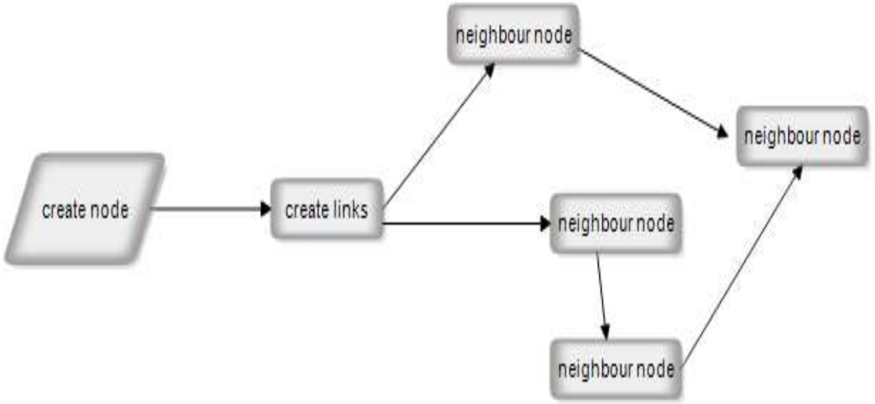
MODULES DESCRIPTION:

- **1.LINK SINGATURE**
- **2. TRAINING SEQUENCE**
- **3. MULTIPLE SINGATURES**
- **4.DETECTING PACKET**

LINK SINGATURE:

- Link signature uses the distinctive wireless channel characteristics between a transmitter and a receiver to produce authentication of the wireless channel.
- we've an inclination to start our investigation with the link signature theme.

- It's assumed that associate wrongdoer “cannot ‘spoof’ associate discretionary link signature” that the wrongdoer “will not have a similar link signature at the receiver unless it's at exactly a similar location as a result of the legitimate transmitter”.

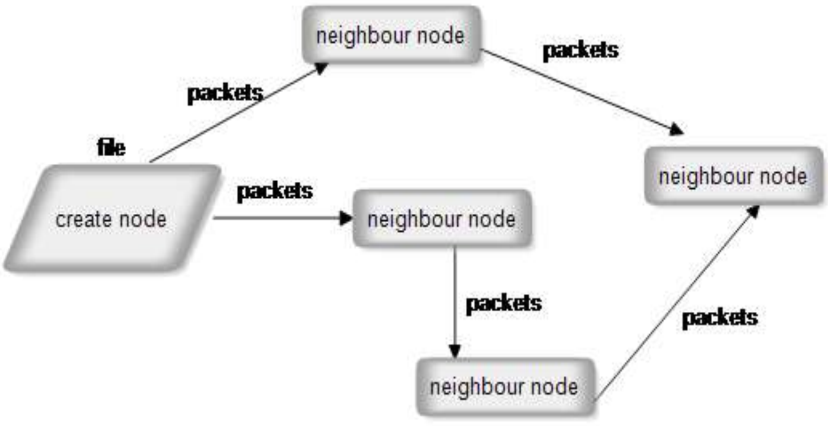


TRAINING SEQUENCE:

- The transmitter initial sends a sequence of bits over the wireless channel.

- The receiver then uses the coaching sequence and therefore the received corresponding packets to estimate channel impulse responses, wherever the information worth of the coaching sequence may be pre-shared.

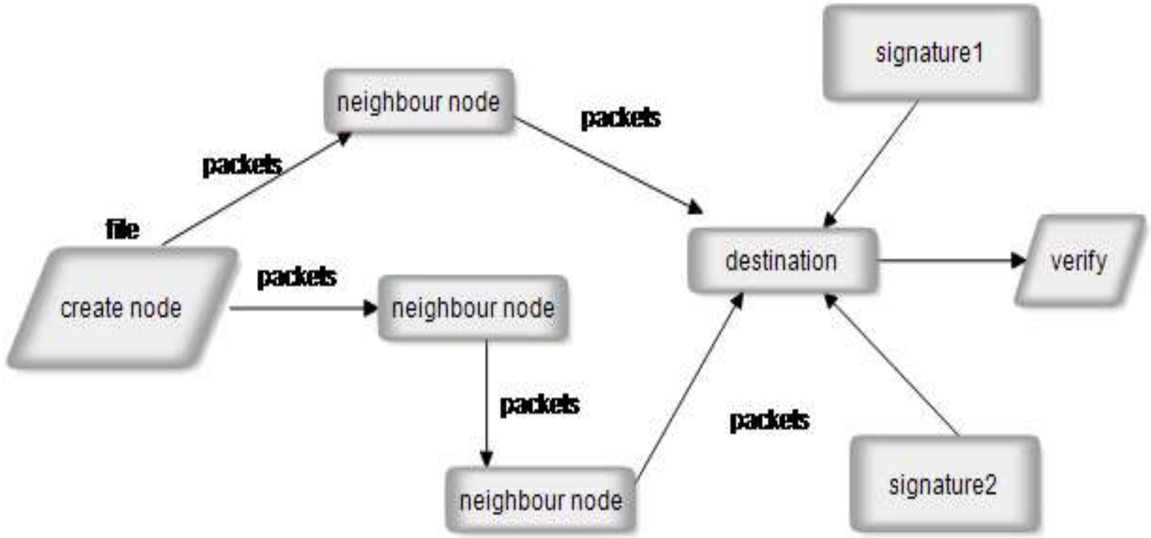
- To transmit the coaching sequence, the transmitter converts files into packets. The transmitter then sends the M symbols to the wireless channel.



MULTIPLE SINGATURES:

- During this paper, we tend to mentioned the final case once each the receiver and therefore the wrongdoer have multiple antennas, and discovered that the mimicry attack remains possible in MIMO systems, as long because the wrongdoer will utilize a minimum of constant range of antennas because the receiver.

- We conjointly extended mimicry attacks to the multiple tone inquisitory based mostly link signature and showed that mimicry attacks will build all existing link signature schemes vulnerable.

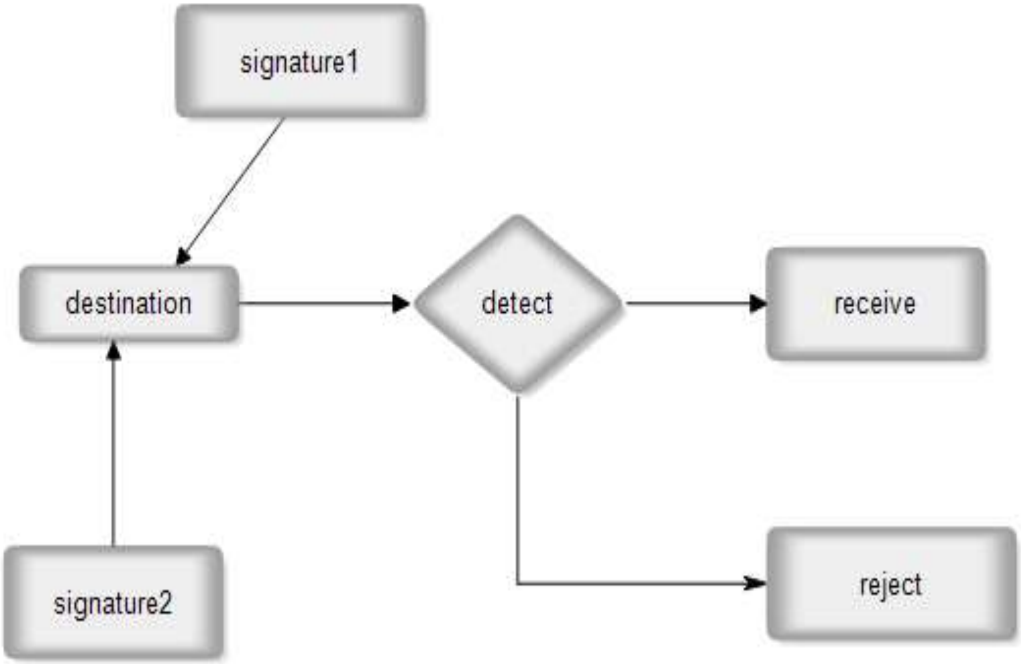


DETECTING PACKETS:

- The assaulter will receive and analyze the Transmitter’s signal to find out the coaching sequence. If the voucher cannot receive the first transmission (e.g., attributable to jam-and-replay attack), the assaulter will still forge link signatures by manipulating and forwarding a frame received from the Transmitter.

- we tend to assume that the Transmitter will use documented time stamping techniques to make sure that the timestamp exactly represents the purpose in time once the SFD field is transmitted in air.

- As a result, upon receiving a frame, the voucher will use the timestamp enclosed within the frame and also the time once it receives the frame, that ought to even be obtained through Medium Access management (MAC) layer time stamping to estimate the traveling time of the frame.



CONCLUSION:

- In this paper, we tend to known the mimicry attack against the existing wireless link signature schemes. we tend to then extended the mimicry attack in MIMO systems and ended that the attacker utilizing a minimum of an equivalent variety of antennas because the receiver's antennas will with success launch the mimicry attack. To defend against the mimicry attack, we tend to projected the novel time-synched link signature construction by desegregation cryptologic protection and time issue into wireless physical layer features. we tend to conjointly performed an in depth set of experiments to demonstrate each the practicability of mimicry attacks and also the effectiveness of time-synched link signature.

REFERENCES:

1. D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks inwireless networks using signalprints," in *Proc. ACM Workshop WirelessSecur. (WiSec)*, 2006, pp. 43–52.
2. N. Patwari and S. K. Kasera, "Robust location distinction using temporal
3. link signatures," in *Proc. 13th Annu. ACM Int. Conf. Mobile Comput.Netw. (MobiCom)*, 2007, pp. 111–122.
4. J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancingwireless link signatures for location distinction," in *Proc. 14th ACMInt. Conf. Mobile Comput. Netw. (MobiCom)*, 2008, pp. 26–37.
5. S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radiotelepathy:Extracting a secret key from an unauthenticated wireless channel,"in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom)*, 2008, pp. 128–139.

6. Z. Li, W. Xu, R. Miller, and W. Trappe, “Securing wireless systems via lower layer enforcements,” in *Proc. ACM Workshop Wireless Secur. (WiSec)*, 2006, pp. 33–42.
7. Y. Liu, P. Ning, and H. Dai, “Authenticating primary users’ signals in cognitive radio networks via integrated cryptographic and wireless link signatures,” in *Proc. IEEE Symp. Secur. Privacy (S&P)*, May 2010,pp. 286–301.
8. K. Zeng, K. Govindan, and P. Mohapatra, “Non-cryptographic authentication and identification in wireless networks,” *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, Oct. 2010.
9. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca,“Ensemble: Cooperative proximity-based authentication,” in *Proc. 8thInt. Conf. Mobile Syst., Appl., Services (MobiSys)*, 2010, pp. 331–344.
10.]Ettus Research. *The USRP Product Family Products andDaughter Boards*, accessed on Apr. 2011. [Online]. Available:http://www.ettus.com/products
11. *GNU Radio—The GNU Software Radio*, accessed on Sep. 2014.[Online]. Available: http://www.gnu.org/software/gnuradio/[15] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.:Cambridge Univ. Press, 2005.
12. R. Safaya. *A Multipath Channel Estimation Algorithm Using a KalmanFilter*, accessed on Apr. 2011. [Online]. Available: http://www.ittc.ku.edu/research/thesis/documents/rupul_safaya_thesis.pdf
13. M. Biguesh and A. B. Gershman, “Training-based MIMO channelestimation: A study of estimator tradeoffs and optimal training signals,”*IEEE Trans. Signal Process.*, vol. 54, no. 3, pp. 884–893, Mar. 2006.
14. K. S. Shanmugan and A. M. Breipohl, *Random Signals: Detection,Estimation and Data Analysis*. New York, NY, USA: Wiley, May 1988.
15. O. Edfors, M. Sandell, J. J. van de Beek, S. K. Wilson, andP. O. Börjesson, “OFDM channel estimation by singular value decomposition,”*IEEE Trans. Commun.*, vol. 46, no. 7, pp. 931–939, Jul. 1998.
16. X. He, H. Dai, W. Shen, and P. Ning, “Is link signature dependable forwireless security?” in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 200–204.