An Improved Wireless Channel Authentication using Multi-Channel Safety Link Signature for Wireless Networks

Prof. P.Gnanasekaran [1], B.Karthika [2]

[1]*Research Guide, Department of Computer Science, Jairam Arts & Science College, Karur, Tamilnadu, India-639003*
[2] *MPhil Scholar, Department of Computer Science, Jairam Arts & Science College, Karur, Tamilnadu, India-639003*

Abstract: *The wireless channel authentication is important for many application areas. The secure authentication mechanisms in wireless networks in order to assistant a node to a secure channel communication is not an easy task due to the limitations of network channel congestion. In exiting wireless link signature techniques used in physical layer authentication mechanism, which uses the unique wireless channel characteristics between a sender and a receiver to provide authentication of wireless channels Wireless multi-channel safety link signature is a physical layer authentication mechanism, which uses the unique wireless channel characteristics between a sender* and a receiver to provide authentication of wireless channels. A defencelessness of existing link signature schemes has been identified by introducing a new attack, called mimicry attack. The propose system improved multi-hop channel authentication algorithm using elliptic curve cryptography algorithm for wireless channel authentication networks. The multiple secure authentication security can improve the security of the network environment. The experimental results demonstrate the effectiveness of link signature based on elliptic curve cryptography.

Keywords-*secure authentication mechanisms; Wireless link signature; safety link signature; multi-hop channel authentication*

I. Introduction

Location distinction in wireless networks aims to detect a wireless user’s location change, movement or facilitate location based authentication. Enforcing location distinction is important for many wireless applications. Location distinction using wireless physical layer information has been extensively studied during the past several years. Scientists have discovered that wireless channel characteristics become uncorrelated every half carrier wavelength over distance (spatial uncorrelation property). This property has been widely explored and adopted to enforce location distinction of wireless devices. Specifically, changes of wireless channel characteristics have been utilized to identify location changes of a wireless transmitter. To discover a new attack against all existing location distinction approaches built on the spatial uncorrelation property of wireless channels. By launching such an attack, the adversary can generate any chosen wireless channel characteristics at a target receiver to deteriorate the location distinction capability of the receiver. The key idea of the discovered attack is to create a virtual multipath channel as undetectable camouflage to make the receiver believe a specified channel characteristic chosen by the attacker.

Among the recent advances in wireless physical layer security is (wireless) link signature. Link signature uses the unique wireless channel characteristics (e.g., the multi-path effect) between a transmitter and a receiver to provide authentication of the wireless channel. Three link signature schemes have been proposed so far. Since its introduction, link signature has been recognized as a wireless channel authentication mechanism for applications where wireless channel characteristics are unique.

A vulnerability of existing link signature schemes has been identified by introducing a new attack called mimicry attack. Traditional link signature schemes assumed that “an attacker cannot ‘spoof’ an arbitrary link signature” and that the attacker “will not have the same link signature at the receiver unless it is at exactly the same location as the legitimate transmitter”. However, a mimicry attacker can forge an arbitrary link signature as long as it roughly knows or can estimate the legitimate signal at the receiver’s location, and the attacker does not have to be at exactly the same location as the legitimate transmitter in order to forge its link signature.

Existing location distinction approaches have been focused on exploiting the spatial uncorrelation property of wireless channels. These approaches demonstrated their success in various wireless scenarios, especially for the high-frequency systems (e.g., WiFi networks) that feature a very short electromagnetic wavelength. However, two recent studies identified a vulnerability of these approaches, and discovered that the wireless spatial uncorrelation property may be violated in a poor multipath environment (e.g., strong line-of-sight path). A further attempt to attack location distinction systems using channel impulse responses. The authors found that a third-party attacker may impersonate Alice to Bob by mimicking the channel impulse response of the wireless link between them, and the authors named such attacks as mimicry attacks.

II. Related Work

The ability of a receiver to determine when a transmitter has changed location is important for energy conservation in wireless sensor networks, for physical security of radio-tagged objects, and for wireless network security in detection of replication attacks. In this paper, we propose using a measured temporal link signature to uniquely identify the link between a transmitter and a receiver. The attacks differ in technical design methodology. The essential way of mimicry attacks is to manipulate the training signal such that the receiver believes an impersonated channel impulse response. Such a manipulation at the training signal level fools the receiver to accept an incorrect channel estimate, but the data payload after the training signal still goes through the real channel. As a result, the receiver will use an incorrect channel estimate to compensate the real channel effect, leading to incorrect packet decoding. In contrast, the virtual multipath attack uses a delay-and-sum process (with chosen weights) to create a virtual channel and pass all the data (e.g., training sequence and data payload) to be transmitted through this virtual channel. The receiver then not only gets a faked channel impulse response, but also uses it to successfully decode the entire data payload. Hence, the design methodology of virtual channel attacks ensures more stealthiest and consistency to fool the receiver.

The simplicity of the delay-and-sum process, as discussed earlier, the virtual multipath attacks can be interestingly extended to enhance the wireless security. For example, researchers have proposed to establish a key between two wireless devices using the channel impulse responses between them. Such a key is totally determined by the wireless physical layer feature and cannot be easily manipulated by the users. The idea of virtual channel attacks can be utilized here to enable the transmitter to control and update the shared key periodically and provide a rich set of shared keys among wireless users. Such attacks can also enable anonymous communications by protecting location privacy of wireless users via virtual channel camouflage.

Location distinction is the ability to determine when a device has changed its position. We explore the opportunity to use sophisticated PHY-layer measurements in wireless networking systems for location distinction. We first compare two existing location distinction methods - one based on channel gains of multi-tonal probes, and another on channel impulse response. Next, we combine the bene fits of these two methods to develop a new link measurement that we call the complex temporal signature. Due to the broadcast nature of the wireless medium, wireless networks are especially vulnerable to Sybil attacks, where a malicious node illegitimately claims a large number of identities and thus depletes system resources. Wireless link signature is a physical layer authentication mechanism, which uses the unique wireless channel characteristics between a transmitter and a receiver to provide authentication of wireless channels. A vulnerability of existing link signature schemes has been identified by introducing a new attack, called mimicry attack.

Although conventional cryptographic security mechanisms are essential to the overall problem of securing wireless networks, these techniques do not directly leverage the unique properties of the wireless domain to address security threats. The properties of the wireless medium are a powerful source of domain-specific information that can complement and enhance traditional security mechanisms. To address the increasing demand for wireless bandwidth, cognitive radio networks (CRNs) have been proposed to increase the efficiency of channel utilization; they enable the sharing of channels among secondary (unlicensed) and primary (licensed) users on a non-interference basis. A secondary user in a CRN should constantly monitor for the presence of a primary user’s signal to avoid interfering with the primary user. Data based channel estimation methods offer low complexity and good performance and are thus quite widely used in communications systems today. But they are also wasteful of bandwidth since they use training sequences to estimate the channel.

Physical-layer key extraction techniques attempt to derive a shared symmetric cryptographic key between two wireless devices based on the principle of channel reciprocity, which states that the signal envelope between two communicating devices is strongly correlated. A key security assumption made in previous literature is that the signal envelope observed by an adversary located greater than a half-wavelength away is uncorrelated with that shared between the two communicating devices; however, this assumption has yet to be rigorously evaluated in previous work on physical-layer key extraction. Wireless link signature is a physical layer authentication mechanism, which uses the multi-path effect between a transmitter and a receiver to provide authentication of wireless signals. We identify a new attack, called mimicry attack, against the wireless link signature scheme. It is assumed in the past that an attacker cannot "spoof" an arbitrary link signature and that the attacker will not have the same link signature at the receiver unless it is at exactly the same location as the legitimate transmitter. Securing communications requires the establishment of cryptographic keys, which is challenging in mobile scenarios where a key management infrastructure is not always present. In this paper, we present a protocol that allows two users to establish a common cryptographic key by exploiting special properties of the wireless channel: the underlying channel response between any two parties is unique and decorrelates rapidly in space. The broadcast nature of a wireless link provides a natural eavesdropping and intervention capability to an adversary. Thus, securing a wireless link is essential to the security of a wireless network, and key generation algorithms are necessary for securing wireless links. However, traditional key agreement algorithms can be very costly in many settings, e.g. in wireless ad-hoc networks, since they consume scarce resources such as bandwidth and battery power.

This dissertation deals with the utilization of channel knowledge in improving the performance of wireless communication systems. The first part is about energy harvesting networks. The transmission policies in energy harvesting wireless systems need to adapt to the harvested energy availability and the channel characteristics. 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.

III. Proposed Approach

Large scale multi-hop wireless networks, which is due to the limited number of cryptographic operations regardless of the number of hops separating the communicating nodes. In addition, it combines several aspects of security, from designing secure protocols to evaluating the implementation of our solution, going through formal automatic analysis of security and overhead of protection analysis. Mobile Networks offer unrestricted mobility devoid of any underlying infrastructure. Typically, mobile networks are deployed in un-trusted environments. Such networks in this day and age have to keep privacy and security of data as a top concern, because eaves dropping peaks here. The root cause behind such eavesdropping is the un-authenticated access of base station on nodes. The eventual outcome is the menace of insecure environment, information misuse, and so on. Cryptosystem is an important technique to identify the authenticity in order to protect the confidential and sensitive data in mobile networks. This paper proposes a simple and efficient authentication protocol for the establishment of secure communication between base station and nodes in mobile networks. The protocol proposed, here, is new one for authentication scheme, having simplicity and efficacy. The protocol is designed by employing a most familiar public-key cryptographic scheme, elliptic curve cryptography and then it is dedicated to mobile networks for authentication of base station. Usage of this protocol in mobile networks will allow only the authorized base station to access the node and hence it will deny the information to eavesdroppers when they try to hack or misuse the node.

The contributions can be summarized in the five following points:

1. Design of multi-hop node authentication mechanisms.
2. Formal automatic analysis of our solutions.
3. Implementation on dynamic topology.
4. Evaluation of the overhead of protection of our solutions.
5. Attack detection based on the a priori overhead evaluation.

A. Network Deployment

Mobile network scenario which involves mobile nodes communicating in ad-hoc mode with wireless technology such as Wi-fi. We assume a trusted authority with the right to assign each node a unique identifier and a pair of public and private keys. Nodes are assumed to know the public keys of each other so that they can authenticate messages signed by others. Each node i is assumed to have a unique ID Ni and a corresponding public/private key pair. We assume that each node must pay a deposit C before it joins the network, and the deposit will be paid back after the node leaves if there is no offend activity of the node. a homogeneous network with N nodes where each node communicates with a set of neighboring nodes N(ni), which is assumed to be time-invariant for all nodes ni. We assume a broadcasting communication model where each node transmits its message to all its neighbors simultaneously. A suitable media access control (MAC) protocol is assumed to be implemented so that whenever a node broadcasts its message, it will be received by all its neighboring nodes. We assume the deployed network is connected, i.e., there exists at least one path between any two nodes in the network.

B. Mobility Model

An extension of AODV protocol is proposed in called as the Ad-hoc on demand multipath distance vector routing protocol (AOMDV) which discovers multiple paths during single route discovery process. To measure the protocol performance in mobility two mobility models are simulated using ns-2 simulator and the protocol performance is analysed. Metrics such as throughput, drop packet ratio and average delay are estimated for random walk model and random waypoint model. AOMDV performance for both the mobility models is consistent. With random waypoint model, the throughput is superior with respect to random walk model. Because of pause time the node gets a bit of steadiness which improves its throughput. In Random Walk Mobility Model, the pause time also affects the average delay. With increasing mobility, i.e. when mean node speed increases the average delay increases means the routing protocol performance degrades. Similar is the case for increased load. For both offered load and mobility average delay is constant for random waypoint mobility model.

C. Attacker Model

Let and denote the received symbols from the transmitter and the attacker, respectively. The attacker's goal in the mimicry attack is to make approximately the same as . Thus, when the receiver attempts to extract the link signature from the attacker's symbols , it will get a link signature similar to the one estimated from . The attacker needs to meet two requirements to launch a mimicry attack: First, the attacker needs to roughly know the received symbols . Second, the attacker needs to manipulate its own symbols, such that when the manipulated symbols arrive at the receiver, they are similar to .

D. Channel Analysis

The assume that there are a Transmitter and a Verifier, who share a secret key K that is only known to them. The Transmitter sends physical layer frames to the Verifier, who then verifies if these frames are directly transmitted by the Transmitter. We assume that the attacker can eavesdrop, overhear, and jam wireless communications. However, we assume that the attacker cannot compromise the Transmitter or the Verifier, and thus does not know their secret.

The attacker at least one of these two pieces of information. It is in general very difficult to prevent a passive attacker from receiving signals (and then extracting valid link signatures). However, it is possible to prevent the attacker from knowing the training sequences. Thus, our initial idea is to use unpredictable, dynamic, and authenticated training sequences for extracting link signatures from wireless packets (frames).

To handle this threat, propose to bring "time" into the scheme. here assume the Transmitter and the Verifier have synchronized clocks. (Our scheme will include a time synchronize component to meet this assumption.) The Transmitter may include a timestamp in the transmitted frame, which indicates the time when a particular bit or byte called the anchor (e.g., the Start of Frame Delimiter (SFD) field) is transmitted over the air. We assume that the Transmitter can use authenticated timestamping techniques to ensure that the timestamp precisely represents the point in time when the anchor is transmitted. Upon receiving a frame, the Verifier can use this timestamp and the frame receiving time to estimate the frame traverse time. An overly long time indicates that the frame has been forwarded by an intermediate attacker.

Minimum Frame Length: If a frame is too short, the Verifier may have difficulty seeing the delay caused by a frame repeater. One solution is to pad extra bits into the frame if the frame length is less than a minimum frame length.

E. Secure Routing

The proposed system examines the case of multiple independently misbehaving nodes. There two strategies for the nodes: (a) continuous misbehaviour, and (b) randomly alter between honesty and misbehavior. In either case, here show S can identify, isolate, and locate the misbehaving nodes. The first step is to identify that more than one misbehaving node exists in PSD, which is achieved.

Elliptic Curve Cryptography (ECC) is a public key cryptography method, which evolved from Diffie Hellman. To understanding how ECC works, let's start by understanding how Diffie Hellman works. The Diffie Hellman key exchange protocol, and the Digital Signature Algorithm (DSA) which is based on it, is some asymmetric cryptographic systems in general use today. It was discovered by Whitfield Diffie and Martin Hellman uses a problem known as the Discrete Logarithm Problem (DLP) as its asymmetric operation. The DLP concerns finding a logarithm of a number within a finite field arithmetic system. Prime fields are fields whose sets are prime. In other words, they have a prime number of members. Prime fields turn out to be of great use in asymmetric cryptography since exponentiation over a prime field is relatively easy, while its inverse, computing the logarithm, is difficult. The "Diffie-Hellman Method for Key Agreement" allow two hosts to create and share a secret key.

Mathematically, a proof to this effect is neither known nor thought to be forthcoming. Before wide-scale implementation, it is thus of the utmost importance that an extensive investigation of the true complexity of the problem is done in order to obtain the highest degree of confidence in the security of discrete logarithm based cryptographic systems. Such an investigation is in progress by various researchers around the world.

An elliptic curve key pair is associated with a particular set of domain parameters D = (q, FR, S, a, b, G, n, h). The public key is a randomly selected point Q in the group generated by G. The corresponding private key is d = logGQ. The entity A generating the key pair must have the assurance that the domain parameters are valid. The association between domain parameters and a public key must be verifiable by all entities who may subsequently use A's public key. In practice, this association can be achieved by cryptographic means (e.g., a certification authority generates a certificate attesting to this association) or by context (e.g., all entities use the same domain parameters).

```
Algorithm ECC: generateKeyPair ()
Input: Domain parameters D
Output: Public key Q, private key d
{
Select d= Î R [1, n − 1]
Compute Q = dG
Return (Q, d)
}
```

The problem of computing a private key d from the public key Q is precisely the ECDLP. Hence, it is crucial that the domain parameters D be selected so that the ECDLP is intractable. Furthermore, it is important that the numbers d generated be random in the sense that the probability of any particular value being selected must be sufficiently small to preclude an adversary from gaining advantage through optimizing a search strategy based on such probability. The purpose of public key validation is to verify that a public key possesses certain arithmetic properties. Successful execution demonstrates that an associated private key logically exists, although it does not demonstrate that someone has actually computed the private key nor the claimed owner actually possesses it. Public key validation is especially important in DH based key establishment protocols where an entity A derives a shared secret k by combining the private key with a public key received from another entity B, and subsequently uses k in some symmetric key protocol (e.g., encryption or message authentication). A dishonest B might select an invalid public key in such a way that the use of k reveals information about A’s private key.

```
Algorithm ECC:  validatePublicKey ()
// Input: Domain parameters D, public key Q
// Output: Acceptance or rejection of the validity of Q
{
Check that Q --
Verify that xQ and yQ Î Fp
Check that Q satisfies the EC equation defined by a and b
Verify that nQ = n If (Verification fails) then
Return “Invalid”
Else
Return “Valid”
}
```

There may be much faster methods for verifying that nQ = _ than performing an expensive point multiplication nQ.

Elliptic Curve Encryption Scheme

For an elliptic curve ElGamal encryption, all computations are done in the finite field Fp. The encryption and decryption procedures for the elliptic curve analogue on the basic ElGamal encryption scheme are presented as algorithms ‘encryptECElGamal’ and ‘decrypt ECEl Gamal’ respectively. A plaintext m is first represented as a point Pm, and then encrypted by adding it to kQ, where k is a randomly selected integer, and Q is the intended recipient’s public key. The sender transmits the points C1 = kG and C2 = Pm + kQ to the recipient who uses the private key d to compute dC1 = d(kG) = k(dG) = kQ, and thereafter recovers Pm = C2 − kQ. An eavesdropper who wishes to recover Pm needs to compute kQ. This task of computing kQ from the domain parameters, Q, and C1 = kG, is the elliptic curve analogue of the DH Problem

```
Algorithm encryptECElGamal ()
// Input: EC domain parameters (p, E, G, n),
public key Q, plaintext m
// Output: Cipher text (C1, C2)
{
Represent the message m as a point Pm in E(Fp)
Select k Î R [1, n − 1]
Compute C1 = kG
Compute C2 = Pm + kQ
Return (C1, C2)
}
Algorithm decryptECElGamal ()
// Input: EC Domain parameters (p, E, G, n),
private key d,
cipher text (C1, C2)
// Output: Plaintext m
{
Compute Pm = C2 − dC1
Extract m from Pm
Return (m)
}
```

As in the finite field case, the security of this cryptosystem lies in the fact that if only G and Q are known to the adversary, it is difficult to determine the number of times G has been added to itself to get Q. This property is due to the random additive structure of points.

```
Algorithm ComputeECDHSecretKey()
// Input: EC domain parameters (p, E, G, n)
// Output: Secret key k
{
User A select nA Î R [1, n − 1]
User A compute PA = nAG
User B select nB Î R [1, n − 1]
User B compute PB = nBG
User A calculate k = nAPB
User B calculate k = nBPA
Return k
}
```

Since it is practically impossible to find the private key nA or nB from the public key PA or PB, it is not possible to obtain the shared secret key k for a third party.

IV. Experimental Results

During the simulation, each node starts its journey from a random spot to a random chosen destination. Once the destination is reached, the node takes a rest period of time in second and another random destination is chosen after that pause time. This process repeats throughout the simulation, causing continuous changes in the topology of the underlying network. **PDR** is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source mobile node. It can be evaluated in terms of percentage (%).

This parameter is also called “success rate of the protocols”, and is described as follows:

Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node.

Where X is the throughput, C is the number of requests that are accomplished by the system, and T denotes the total time of system observation.

Average end-to-end delay Average end-to-end delay signifies how long it will take a packet to travel from source to destination node. It includes delays due to route discovery, queuing, propagation delay and transfer time.

Where dend-end= end-to-end delay, dtrans= transmission delay,dprop= propagation delay,dproc= processing delay,dqueue= Queuing delay and N= number of links. This metric is useful in understanding the delay caused while discovering path from source to destination.

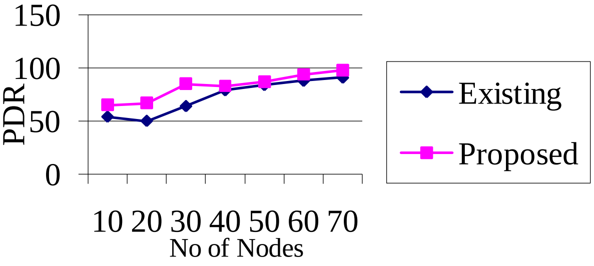

Fig. 2 Compare PDR existing with proposed

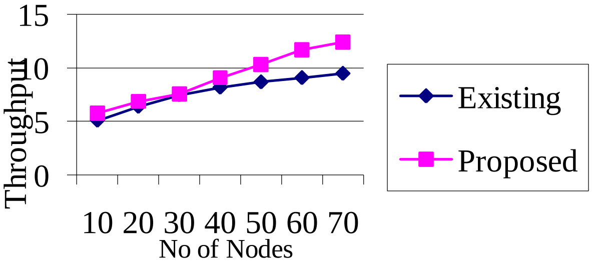

Fig. 3 Compare throughput existing with proposed

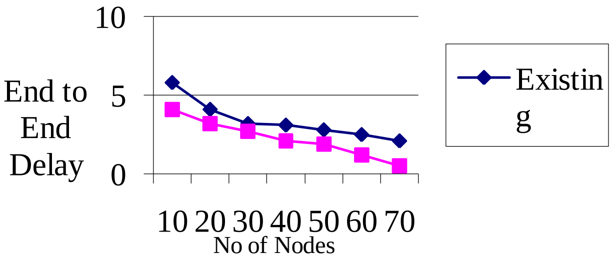

Fig. 4 Compare end to end delay existing with proposed

V. Conclusion

The multi-hop channel authentication algorithm using elliptic curve cryptography algorithm for wireless channel authentication networks. The multiple secure authentication security can improve the security of the network environment. The experimental results demonstrate the effectiveness of link signature based on elliptic curve cryptography. In this proposed security algorithm achieve low cost overhead and low traffic compare with existing algorithm. The proposed experimental result run in simulation environment compare with existing channel authentication system.

References

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

[2] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, “Advancing wireless link signatures for location distinction,” in Proc. of ACM MobiCom ’08, September 2008, pp. 26–37.

[3] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, “Channel based detection of sybil attacks in wireless networks,” IEEE Trans. Information Forensics and Security, vol. 4, no. 3, pp. 492 – 503, 2009.

[4] Y. Liu and P. Ning, “Enhanced wireless channel authentication using time-synched link signature,” in Proc. of IEEE INFOCOM ’12, March 2012.

[5] Z. Li, W. Xu, R. Miller, and W. Trappe, “Securing wireless systems via lower layer enforcements,” in Proc. of ACM WiSe ’06, September 2006, pp. 33–42

[6] 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.

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

[8] R. Safaya, “A multipath channel estimation algorithm using a kalman filter,” Thesis, University of Kansas, 2000.

[9] M. Biguesh and A. B. Gershman, “Training-based mimo channel estimation: A study of estimator tradeoffs and optimal training signals,” IEEE Trans. Signal Processing, vol. 54, no. 3, pp. 884–893, March 2006.

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

[12] J. Xiong and K. Jamieson, “Securearray: Improving wifi security with fine-grained physical-layer information,” in Proc. of ACM MobiCom ’13, 2013, pp. 441–452.

[13] Y. Liu and P. Ning. Mimicry attacks against wireless link signature and defense using time-synched link signature. Technical Report TR-2011- 17, NC State University, Computer Science Department, July 2011.

[14] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radiotelepathy: extracting a secret key from an unauthenticated wireless channel. In Proceedings of the 14th ACM International Conference on Mobile Computing and Networking (MobiCom ’08), 2008.

[15] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener. Robust key generation from signal envelopes in wireless networks. In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS ’07), pages 401–410, 2007.