Non-Cryptographic Authentication and Identification in Wireless Networks

Kai Zeng, Kannan Govindan, and Prasant Mohapatra
Computer Science Department, University of California, Davis, CA 95616
{kzeng, gkannan, prasant}@cs.ucdavis.edu

***Abstract*—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 cross-layer security design concludes this paper.**

***Index Terms*—Wireless ad hoc networks, mobile networks, physical-layer security, authentication, identification**

I. Introduction

Advances in communication and networking technologies are rapidly making ubiquitous network connectivity a reality. Wireless networks are indispensable for supporting such access anywhere and anytime. Due to its "open air" nature, the wireless environment imposes greater challenges on ensuring network security than in wired networks. Because of the broadcast nature of the wireless medium, the communication can be easily eavesdropped or intercepted. The wireless devices can be compromised and modified to behave maliciously or selfishly. These vulnerabilities in wireless networks would undermine the authenticity, confidentiality, integrity, and availability if they are not carefully addressed. On the flip side, the inherent and unique characteristics of the wireless medium or devices can be exploited to enhance the network security [1]–[3].

Among the various types of attacks in wireless networks, identity-based attacks (i.e., MAC address spoofing) are easy to launch and can significantly degrade the network performance. Identity-based attacks are considered as the first step in an intruder's attempt to launch a variety of attacks, including denial of service (DoS), session hijacking, man-in-the-middle, data modification, and sniffing. Although traditional cryptographic techniques can potentially prevent identity-based attacks in wireless networks, they are either inefficient or fall short in certain existing scenarios. A few shortcomings can be identified as follows.

First, although existing 802.11 security techniques provide authentication for data frames, management and control frames are usually not protected. Second, most of the cryptographic techniques are ill suited for a less equipped distributed wireless network due to high complexity and computational requirements. In addition, the conventional cryptographic security mechanisms need key management to distribute, refresh, and revoke the keys. However, key management is difficult in ad hoc networks where nodes join and leave the network frequently. Third, even when the traditional cryptographic means are feasible, wireless devices are subject to physical compromises in an adversarial environment. Any unprotected keying materials used for authentication stored on the device may be compromised through physical attacks, which will diminish the strength of the security mechanisms. Furthermore, in emerging wireless networks, such as cognitive radio networks, the (primary) users shall be identified at the signal level without relying on higher layer cryptographic means.

In light of these circumstances, there is an increasing interest in enhancing or supplementing traditional authentication protocols in wireless networks with various lower/physical layer fingerprint/signature schemes. The existing lower/physical layer signature schemes can be broadly classified into three categories: software based, hardware based, and channel/location based ones. Most of the schemes proposed in the literature are applicable only for static networks. Limited work has considered mobile scenarios. In this paper, we will review and discuss the existing and ongoing research on non-cryptographic authentication/identification in both static and mobile wireless networks. In addition, we propose two RSS based authentication schemes in mobile networks.

This paper is organized as follows. In Section II, we give an overview about different non-cryptographic techniques for user authentication or identification in static networks. Section III presents physical layer assisted

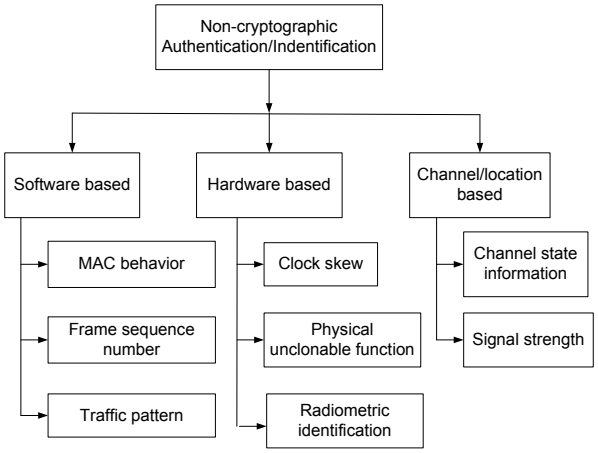


Fig. 1. Classification of non-cryptographic authentication and identification schemes in wireless networks

authentication schemes in mobile networks. Section IV presents summary of the lower/physical layer based authentication schemes. Future work on the cross-layer security for emerging networks is discussed in Section V and concluding remarks are outlined in Section VI.

II. Non-cryptographic Wireless User Authentication and Device Identification

Non-cryptographic wireless user authentication and device identification techniques can be broadly classified into three categories:

- Software based Fingerprinting
- Hardware based Fingerprinting
- Channel/Location based Fingerprinting

A pictorial representation of the different categories of wireless user/device authentication/identification schemes is given in Fig. 1. In this section, we will provide an overview about these schemes.

A. Software based Fingerprinting

Software based fingerprinting techniques are essentially based on the unique characteristics and style of the software programs or protocols running on the devices. IEEE 802.11 standards are de-facto medium access control (MAC) protocols for wireless networks. Due to their large and complex specifications, they are usually implemented in slightly different ways by different device manufacturers and driver developers. These variations in implementations can be exploited as a signature to identify different wireless devices. Depending on the combination of the chipset, firmware, and device driver, different devices may exhibit different MAC layer behaviors. For example, the probe requests sent by wireless nodes vary between manufactures. Frame sequence numbers can also be used to detect presence of multiple 802.11 devices using the same MAC address [4]. The traffic patterns (such as packet sizes and destination addresses) of the wireless users have been exploited to identify different users [1].

Merits: Software based fingerprinting can be easily recorded or extracted using off-the-shelf wireless devices and existing softwares. Specifically, by putting the wireless card into monitor mode and using *tcpdump* or *wireshark*, all the frames sent in the air can be sniffed. Therefore, the frame/beacon interval, frame size, and source and destination addresses of a frame can be obtained easily.

De-merits: The disadvantage of software based fingerprint is that it cannot distinguish between different physical devices running the same software. An adversary may be able to learn the behavior of a genuine user and mimic its behavior by changing its device driver.

B. Hardware based Fingerprinting

Hardware based fingerprinting is the reflection of defects/unique design of the hardware on the transmitted waveforms. Although the hardware based fingerprinting techniques can be broad, we identify three important hardware based fingerprinting techniques in this paper: radiometric fingerprinting, clock skew fingerprinting, and physically unclonable functions.

Radiometric fingerprinting: Radiometric fingerprinting is a recently explored technique to identify the wireless devices uniquely. The underlying assumption in security schemes based on radiometric fingerprinting is that the unique characteristics of a hardware transceiver cannot be replicated or copied from one device to another as how human nature/behavior cannot be replicated.

Radiometric identification can be further classified into two categories: signal transient-based identification and modulation domain based identification [2]. The transient-based approach extracts the transient portion of the signal associated with the start-up period of a transceiver prior to transmission. Since this transient feature reflects the unique hardware characteristics of a transceiver, it can be used to classify different transmitters. The modulation domain based scheme uses a feature space consisting of five distinct features from the modulation domain of the 802.11 frame.

Merits: This signature scheme uses the inherent hardware imperfections and characteristics. It is hard to spoof the signature by using off-the-shelf wireless devices.

De-merits: The disadvantage of the radiometric based signature schemes is that they are vulnerable to impersonation and replay attacks if the attacker is more

powerful. Specifically, if the attacker is a software defined radio (SDR) or high-end arbitrary waveform generator, it can mimic the radiometric features [5]. Furthermore, the schemes are only suitable for the static case, where the signal properties can be reliably extracted without being affected/distorted by other factors, such as mobility or interference. Finally, existing schemes need expensive signal analyzer to profile and verify the radiometric signature. It is likely infeasible to deploy an expensive vector signal analyzer in an unsecured and hostile physical environment.

Clock skew fingerprinting: Clock skew fingerprinting works based on the concept that no two clocks run same. The clocks in the modern day wireless devices are built based on the inexpensive crystal oscillators, which are affected by a number of environmental factors and the aging effects. Therefore, the clocks in wireless devices will always have some skew with respect to the reference clock. This skew is unique on different wireless devices, so it can be used as a signature to identify different wireless devices [6].

Merits: This scheme does not require any additional hardware to realize as it exploits the already existing defects in the clock crystals.

De-Merits: Although the clock skews are different among wireless devices, they are measured based on the report of the true value of the clock. Attackers can mimic the clock skew by manipulating the time-stamps. It is hard to change this signature once an attack is detected.

Physically unclonable functions (PUFs): PUFs are a novel method of generating signatures based on the complex physical characteristics of the ICs in the wireless devices [7]. For instance, a unique signature for a wireless device can be generated based on the random delay characteristics of the wires and transistors in the micro electronic chips of a particular wireless device. An arbiter circuit can be implemented to take the wire delay between different signals as the input and output a unique signal that represents the delay between wires.

Merits: It is hard to mimic the signature obtained with PUFs as the signal characteristics are highly random and influenced by the environmental and location effects.

De-Merits: The disadvantage of this scheme lies in its requirement of specially manufactured ICs in the wireless devices. Such hardware is not widely available and would be expensive or impractical to retrofit onto existing devices. Moreover, it requires to exchange a large number of challenge-response messages. Like the radiometric and clock skew based signature, it is hard to change/mitigate once the attacker mimics the characteristics of the signature.

C. Channel/Location based Fingerprinting

Both channel state information (CSI) and received signal strength (RSS) have been used to identify wireless users or detect identity-based attacks [3], [8]. The CSI commonly indicates the channel impulse response, while RSS is usually determined by both the transmission power and the CSI. The foundation behind these schemes is that the CSI and RSS are location-specific due to path loss and channel fading. An attacker, who is at a different location from the genuine user, will incur different CSI or RSS profiles as observed by monitors/access points. Most works in this category usually assume the users are static. In a mobile scenario, these schemes will generate excessive false alarms.

Based on the fact that wireless channel response decorrelates quite rapidly in space, a physical-layer algorithm is proposed to combine channel probing with hypothesis testing to determine whether current and prior communication attempts are made by the same user (same CSI).

Although CSI provides detailed information about the channel, it is not available in the current device driver, which prevents its practical usage for commodity wireless devices. Instead, a coarser information (i.e. RSS), which is readily available in the current device driver, is widely used in the real systems. A recent mechanism employs the minimum distance testing in addition to cluster analysis to determine the number of attackers and localize them using RSS information [9].

Merits: Channel based fingerprinting schemes exploit the naturally available random and location-distinct characteristics of the wireless channel hence very hard to mimic. The RSS based schemes are easy to implement in the current wireless systems. It has been proven to be effective. Unlike the hardware based schemes, it is easy to tune the characteristics of this signature once the attack is detected.

De-Merits: The approaches might not work well in a highly dynamic environment where the channel state or RSS changes drastically over time. The detection algorithm may need a large number of samples to ensure a desirable performance.

As the channel/location based fingerprinting has relatively better advantage in terms of its uniqueness, adaptiveness and being hard to mimic, we concentrate on the channel based fingerprinting in the rest of this paper. In the following section, we will discuss channel based authentication in a more challenging scenario, i.e., the mobile network.

III. Channel Assisted Authentication in Mobile Wireless Networks

The challenge of using CSI or RSS to assist authentication in a mobile scenario lies in the fact that the CSI or RSS tends to change over time due to the nodes' mobility and changing environment. It is hard to obtain a relatively stable CSI or RSS profile for a mobile node. Hence, it becomes difficult to decide if a CSI or RSS change is due to the node's mobility or an impersonation attack.

A. CSI based Authentication

A recent work proposes an intra-burst and inter-burst authentication framework using CSI in mobile networks [3]. For the intra-burst authentication, the channel responses of the consecutive frames are assumed to be highly correlated. When the difference of the channel responses exceeds some threshold, the receiver will assume the subsequent frame is sent from an attacker. However, the inter-burst authentication is missing in the literature. In the following sections, we will propose two RSS based intra and inter-burst authentication schemes.

B. RSS based Authentication

In the following discussion, we introduce three different parties: Alice, Bob and Eve. Both Alice and Bob are legitimate parties. Without loss of generality, we assume Alice is the initiator of the communication with Bob. Eve is an active attacker who can inject messages into the medium using Alice's identity, i.e., Eve can change her MAC address into Alice's and try to impersonate Alice. Eve can also passively overhear the messages exchanged between Alice and Bob. Bob wants to detect Eve's impersonation attack even when the packet sent from Eve carries the same identity as Alice's.

We have conducted an indoor experiment on the second floor in a campus building, where Bob is sitting in a room, while Alice and Eve are randomly moving on the hallway. All the parties are Dell Latitude E5400 laptops and transmit packets from a fixed antenna. Both Alice and Eve send UDP packets to Bob with an interval of 10ms. The packets from Alice and Eve received by Bob are interleaved with the interval of about 5ms. We consider the *average case* where Eve launches the attack from a random location. The distance between Alice and Eve changes randomly in the range of 0.5m to 20m.

1) RSS similarity based authentication: In RSS Similarity based Authentication (SA), in order to authenticate the n^{th} frame DATA_n, Bob will compare its RSS with that of DATA_{n-1}. If the difference is within a certain range, Bob will assume the signal comes from Alice. Otherwise, he will generate an alarm.

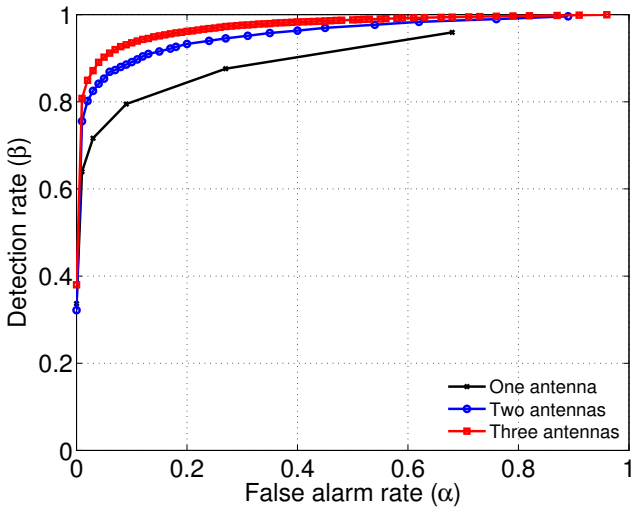


Fig. 3. ROC of SA in an indoor test under average case with packet interval of 10ms

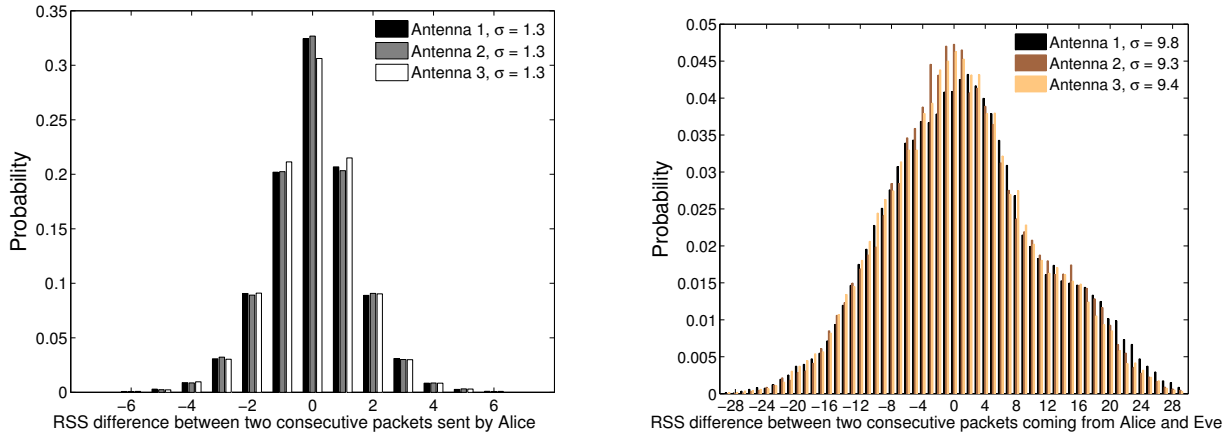
Most of the recent 802.11 devices have two (or more) antennas to support diversity. Specifically, in our experiment, the laptops are equipped with three antennas. Therefore, for each data received by Bob, he can observe three RSS values. This increased dimension of RSS readings can help Bob to detect an impersonation attack more accurately.

Similar to the intra-burst authentication in [3], the SA can be formulated as a hypothesis test. We can apply Neyman-Pearson hypothesis test to evaluate the tradeoff between false alarm rate and detection rate.

Fig. 2 shows the probability distribution of the RSS changes with/without attack in the indoor test. The RSS change is mainly determined by the large scale path loss or distance difference between the Alice-Bob link and Eve-Bob link when there is an attack. Therefore, the RSS changes on Bob's three antennas should be modeled as identically correlated Gaussian distribution under attack. However, the changes can be modeled as independent and identically distributed (i.i.d.) Gaussian without attack due to the spatial diversity. The RSS changes are much larger or more variable under an attack than no attack as shown in Fig. 2.

We use the receiver operating characteristic (ROC) curve for performance evaluation. ROC is a classical method for representing the trade-off between false alarm rate (α) and detection rate (β). Fig. 3 shows the ROC obtained from the indoor experiment. It shows that multiple antenna diversity improves the performance of SA.

We also conducted *worst case* experiment, where Eve



(a) Probability distribution of RSS changes observed at Bob's three antennas without attack

(b) Probability distribution of RSS changes observed at Bob's three antennas under attack

Fig. 2. RSS changes between consecutive frames without attack (all frames coming from Alice received by Bob) and under attack (each frame coming from Alice and Eve respectively) in an indoor test with packet interval of 10ms in the average case

shadows Alice within 0.5m. We found that it is harder for Bob to distinguish Alice from Eve. We obtained 74% detection rate with 5% false alarm rate when Bob uses three-antenna RSS information. To improve the performance of SA in this worst case scenario, Bob needs either more antennas to increase the dimension of the RSS information or finer-grained CSI.

2) Temporal RSS variation authentication (TRVA): When the time interval between two consecutive frames is larger than some threshold, or the sender already moved to another location, the RSS of the received DATA becomes uncorrelated with the previous one. In such situations, we apply TRVA scheme, in which Alice will send Bob a list of RSS variations of ACK frames she received in her previous communication with Bob. If this observation is similar to Bob's version, then Bob will assume it is Alice. Otherwise, Bob will trigger an alarm.

TRVA is motivated by the wireless channel reciprocity principle, which has been recently exploited to generate a secret key between two parties [10]. Reciprocity principle indicates that the channel state between two transceivers should be identical at any instant of time. The RSS is mainly determined by the channel state (may also be affected by ambient noise or measurement error) and transmission power. Intuitively, when Alice and Bob transmit at the same power, they suppose to observe similar RSS variations.

We define the *temporal RSS variation* with lag k ($k > 1$) as:

$$\Delta S(n,k) = S(n) - S(n-k) \quad (1)$$

where $S(n)$ and $S(n-k)$ are the RSS of the n^{th} and $(n-k)^{th}$ DATA frames received by Bob or the corresponding ACK frames received by Alice. In order to authenticate DATA_n to Bob, Alice sends Bob the temporal RSS variation list corresponding to the ACK frames she received from their previous communication. For example, Alice can construct a list consisting of three temporal RSS variations as $[\Delta S(n-1,k),\ \Delta S(n-1-g-k,k),\ \Delta S(n-1-2g-2k,k)]$, where g is a guard parameter. Bob can generate the corresponding list based on his observation.

In Eq. (1), if the unit of RSS is dbm, the temporal RSS variation is transmission power independent, since the transmission power effect is canceled when we subtract RSS in dbm. Therefore, even when Alice and Bob transmit at different power, they should also observe similar RSS variations.

Attack model for TRVA. There are two attack models considered for TRVA: *eavesdropping attack* and *replay attack*. In the eavesdropping attack, Eve will overhear the channel, and measure the RSS of the ACK frame sent from Bob to Alice. She generates the temporal RSS variation list based on her measurement using the same method as Alice and Bob, and sends the list to Bob hoping on passing the authentication. In the replay attack, Eve replays Alice's RSS variation list to Bob.

3) Performance of TRVA: Fig. 4 shows the ROC of TRVA under the indoor test with different lags and list lengths. The guard parameter g is fixed at 3. We can observe that for the same lag, longer list lengths improve the detection performance. Similarly, for the same list length, larger lags provides better performance. With

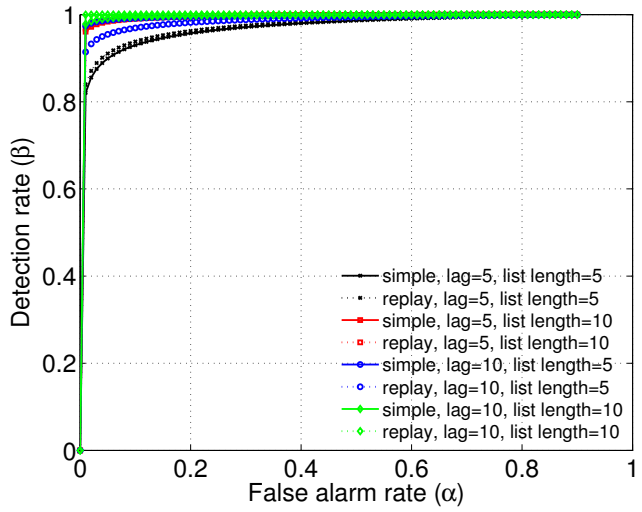


Fig. 4. ROC of TRVA under an indoor test in the average case with packet interval of 10ms ('simple' denotes eavesdropping attack and 'replay' denotes replay attack).

larger lags, the variation would be more unpredictable and variable. However, the list length plays a more important role. As we can see, TRVA performs better when lag = 5 and list length = 10 than the case when lag = 10 and list length = 5. We found that when g is less than 3, which implies 30ms packet interval, the consecutive variations may be correlated. But when it is larger than 3, they are nearly uncorrelated (i.e. the correlation coefficient is less than 0.1).

We also observed that even when Eve shadows Alice within 0.5m, TRVA can achieve 99% detection rate with 5% false alarm rate in the indoor test under the eavesdropping and replay attacks. It is well consistent with the theory that when Eve is several wavelengths away from Alice, the channel variations she observes should be uncorrelated with that of Alice's.

C. Applicability of SA and TRVA

The SA is based on the assumption that the channel state or RSS of consecutive DATA packets are highly correlated. This correlation is usually indicated by the channel coherence time, during which the channel state is considered to be stable or predictable. In 802.11 system, if we assume a walking speed of 1m/s and the carrier frequency of 2.4GHz, we can calculate that the channel coherence time is about 53ms. However, when the moving speed is increased, the channel coherence time is shortened. For example, in a driving scenario with speed of 10m/s, the channel coherence time is 5.3ms. In this case, the packet interval may not be shorter than the channel coherence time, thus SA may not work well in a highly mobile scenario.

The SA scheme is based on the assumption that the DATA_{n-1} is already authenticated when Bob is going to authenticate DATA_n. We note that at the outset of this scheme, in order for Bob to get an initial RSS for Alice, it may be necessary to employ a higher-layer authentication protocol to bootstrap the association between Alice and a corresponding RSS. However, this is a one-time procedure.

The applicability of TRVA is largely dependent on the reciprocity. In practice, since the radio is half-duplex, the bidirectional Alice and Bob channel cannot be measured at the same time. Specifically, in our scheme, the RSS of DATA and ACK cannot be measured simultaneously. However, the time difference between the two measurements is about 0.5ms assuming a transmission rate of 12Mbps and packet size of 512 bytes. This time difference is much smaller than the channel coherence time even in a highly mobile scenario. Therefore, TRVA should work well in a more dynamic scenario.

The TRVA scheme assumes that all the DATA whose RSS is used in calculating the variation list are already authenticated. These DATA can be authenticated by the SA scheme, or some higher-layer authentication protocol. TRVA requires Alice to send extra information, the variation list. Therefore, we consider TRVA as a more expensive authentication scheme than SA.

Note that, SA and TRVA can be used in the scenario even when cryptographic mechanisms, such as HMAC (Hash-based Message Authentication Code), are available. For example, when the authentication key used by HMAC is compromised, SA and TRVA can be used as a complementary authentication mechanism to verify the identity of the sender. Furthermore, SA introduces less communication and computation overhead than traditional cryptographic mechanisms. Specifically, SA does not need the sender to append any authentication code with the message. It only requires the receiver to cache the RSS information of the previous received DATA. Depending on security strength, TRVA may also introduce less communication overhead than cryptographic mechanisms. For example, if each RSS variation is represented by a byte, TRVA only needs to append a 10-byte variation list to achieve desirable authentication strength as shown in Fig. 4. However, HMAC needs 20 bytes if SHA-1 is used. Both SA and TRVA are more computationally efficient than HMAC since they use simple Neyman-Pearson test. For storage, TRVA introduces extra overhead than traditional cryptographic mechanisms, since it requires both the sender and receiver to cache RSS variation list.

IV. Summary of non-cryptographic authentication and identification schemes

A. Advantages

The non-cryptographic authentication and identification schemes can be used to augment or enhance the existing cryptography based mechanisms. These schemes exploit the inherent defects/characteristics of the devices or wireless channel to extract fingerprints. Among the software, hardware, and channel based signature schemes, channel based fingerprinting is most robust in terms of its uniqueness, location distinction, adaptiveness and being hard to mimic.

B. Limitations

Although these schemes can be used to detect identity-spoofing attacks or to authenticate/identify a particular user, they cannot achieve 100% detection rate without introducing false alarm. There is always a trade-off between the detection rate and false alarm rate in these schemes. Furthermore, most of the schemes are only applicable in static cases, where the device, signal, or channel characteristics are relatively stable. Although CSI and RSS based authentication schemes are proposed for mobile networks, the trade-off between the detection rate and false alarm rate still remains.

To mitigate these shortcomings, a holistic cross-layer approach using multiple layer information combining with traditional cryptographic means are desirable as explained in the next section.

V. Further Research Scope

So far the proposed authentication schemes are based on either cryptography or physical layer information. An integration of these two primitives are desirable to secure the emerging wireless networks. For example, in highly dynamic networks, such as mobile ad hoc networks, vehicular ad hoc networks, or delay tolerant networks, it is hard to maintain a central authority to efficiently distribute and manage the key. Therefore, users without any pre-established contact have to initialize a shared secret or associate to each other on-the-fly. Traditional cryptography based Diffie-Hellman key exchange technique can serve for this purpose. However, it is subject to man-in-the-middle attack. In order to prevent the man-in-the-middle attack, two parties usually rely on a shared secret. Thus, it brings the dilemma that Diffie-Hellman is used to generate a shared key between two parties, but in order to prevent the man-in-the-middle attack, we need a pre-shared secret between the two parties. A possible and promising solution to this problem can be

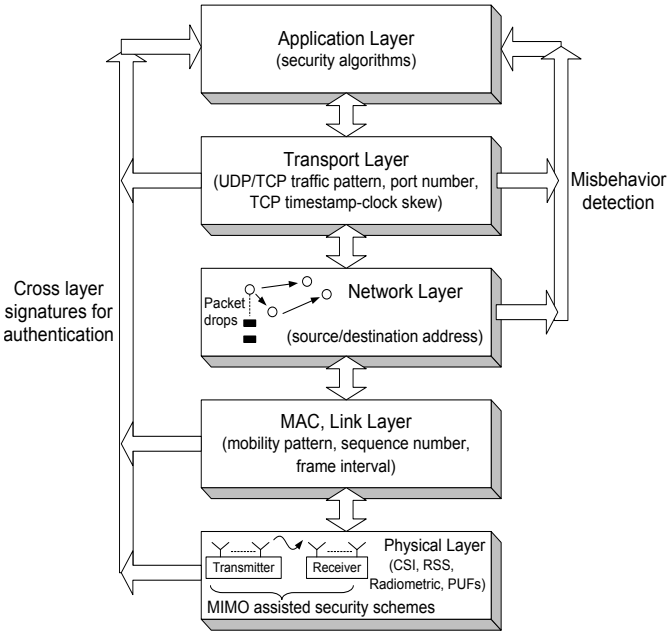


Fig. 5. Cross layer security schemes

a cross-layer security design. By exploiting the unique properties of the wireless channel, the two parties can somehow identify or authenticate the message exchanged in the Diffie-Hellman protocol without relying on a pre-shared key. For example, Alice knows it is Bob sending the Diffie-Hellman key exchange messages to her when she observes a signal characteristic associated with these messages, and this characteristic can only be induced at a particular location where Bob is at.

For intrusion or malicious behavior detection, it is also desirable to examine multiple layer information to improve the probability of detection. The dependency and correlation between multiple layer behaviors or observations can be used to detect malicious/selfish nodes. An illustrative example of a cross layer signature scheme for authentication as well as misbehavior detection is given in Fig. 5. Physical layer CSI/RSS/radiometric information and emerging technologies, such as MIMO (multiple-input and multiple-output) can be combined with the MAC layer sequence number/frame interval/mobility pattern and Transport layer TCP time stamp/traffic pattern/port number to generate a strong authentication scheme to authenticate a node. For misbehavior detection, network layer source address and destination address can be used along with the transport layer traffic patterns.

VI. Conclusion

In this paper, we provided an overview about various non-cryptographic means for user authentication and de-

vice identification in both static and mobile wireless networks using lower/physical layer properties or information. We discussed advantages as well as limitations of these schemes and their implementation issues. Although most of the existing schemes show their usefulness in static wireless networks, limited efforts have considered mobile cases. To advance the existing research, we proposed two RSS based authentication schemes in mobile networks. We conclude that a holistic cross-layer security approach using multiple layer information combining with traditional cryptographic mechanisms are desirable in emerging wireless networks.

REFERENCES

[1] J. Pang, B. Greenstein, R. Gummadi, S. Seshan, and D. Wetherall, "802.11 user fingerprinting," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking MobiCom '07*, 2007, pp. 99–110.

[2] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in *Proceedings of the 14th ACM international conference on Mobile computing and networking MobiCom '08*, 2008, pp. 116–127.

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

[4] F. Guo and T. Chiueh, "Sequence number-based MAC address spoof detection," in *Proceedings of 8th International Symposium on Recent Advances in Intrusion Detection (RAID)*, 2005, pp. 309–329.

[5] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy, "Attacks on physical-layer identification," in *WiSec '10: Proceedings of the third ACM conference on Wireless network security*, 2010, pp. 89–98.

[6] S. Jana and S. K. Kasera, "On fast and accurate detection of unauthorized wireless access points using clock skews," in *Proceedings of the 14th ACM international conference on Mobile computing and networking MobiCom '08*, 2008, pp. 104–115.

[7] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th ACM annual Design Automation Conference DAC '07*, 2007, pp. 9–14.

[8] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *The 13th annual ACM international conference on mobile computing and networking, MobiCom*, 2007, pp. 111–122.

[9] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Determining the number of attackers and localizing multiple adversaries in wireless spoofing attacks," in *The 28th Conference on Computer Communications Infocom*, 2009, pp. 666–674.

[10] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *IEEE Infocom 2010*, March 2010.