International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 8 – MAY 2017.

PREVENTION OF MIMICRY ATTACKS USING SECULAR CERTIFIED ECC AUTHENTICATION MECHANISM

K.Rajammal [#1] and Antony Mutharasan [*2]

[#] *Research Scholar, Department of CS, Sardar Raja College of Engineering, Tirunelveli, India*

[*] *Asst Professor, Department of CSE, Sardar Raja College of Engineering, Tirunelveli, India*

***Abstract*— The technologies in Wireless environments impressed a lot of people in recent years. Due to its distributed nature, the adoptions of Wireless physical layer security are rapidly growing in both indoor and outdoor wireless environments. Concurrently, it is more sensitive towards the security threats that degrade the network performance. The advent of multipath routing system, especially in Multiple Input Multiple Output systems, throws a novel attack, named, mimicry attacks. Mimicry attacks are the attacks that are caused by the actions of illegitimate users, in which they pretend as the legitimate transmitters/ receivers. In previous work, time-based link signature scheme is executed which fails to yield better performances. In this paper, we propose an improved Elliptical Curve Cryptography algorithm which is achieved by two-step authentication framework using secular certified systems. All the security aspects of real-time applications were fulfilled by our proposed scheme. The main contribution is the improvisation of the authentication phase between legitimate and illegitimate users. Experimental results will prove the efficiency of our proposed scheme.**

Index Terms*— Link signature, MIMO, Elliptical Curve Cryptography

I. INTRODUCTION

Wireless physical layer security is becoming increasingly important as wireless devices are more and more pervasive and adopted in critical applications. There have been multiple proposals in recent years to provide enhanced wireless security using physical layer characteristics, including fingerprinting wireless devices, authenticating and identifying wireless channels, and deriving secret keys from wireless channel features only observable to the communicating parties. 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.

In this paper, we identify the mimicry attack against these link signature schemes. Link signature based wireless security mechanisms exploit the radio channel characteristics between two wireless devices to provide security protection complementary to traditional cryptographic approaches. The success of these schemes relies crucially on the uniqueness of link signatures resulting from the assumed fast spatial decorrelation of wireless channels; in particular, it is widely accepted that half a wavelength separation is sufficient for security assurance. Built upon this optimistic assumption, various secret key extraction and signal authentication techniques have been developed based on link signatures (e.g., [1–8]). However, two critical questions remain unclear. First, does the common "half-wavelength decorrelation" assumption hold in all circumstances? As pointed out in [9–11], the spatial channel correlation is significantly influenced by the angular spread (AS) of the incoming signal. When two receivers are surrounded by rich scatterers, their corresponding AS is usually large and the half-wavelength decorrelation conclusion holds. But when a line-of-sight (LOS) component exists or the waveguide propagation effect dominates, the AS is small and will induce high spatial channel correlation. In fact, high spatial channel correlations have already been observed in real world experiments [12].

Second, when the half-wavelength decorrelation assumption is violated, is the current link signature technique still able to provide security protection to wireless applications. This question attracts research interest very recently (e.g., [13, 14]). However, to the best of our knowledge, none of the existing literatures answers it in quantifiable measures based on a solid analysis. The mimicry attack can apply to the following example scenarios when link signatures are used for authentication:

(1) launching location spoofing attacks: an attacker can utilize a fake location to fool a target receiver by creating a fake wire-less link signature.

(2) bypassing motion detection systems: an attacker could maintain its wireless signature unchanged while it is actually moving, thus from the perspective of the target receiver, who utilizes the wireless link signature to determine whether the transmitter moves or not, the attacker appears to remain stationary.

(3) Bypassing wireless transmitter authentication systems: an attacker can impersonate a legitimate transmitter by forging its wireless link signature.

In fact, high spatial channel correlations have already been

observed in real world experiments [12]. Second, when the half-wavelength decorrelation assumption is violated, is the current link signature technique still able to provide security protection.

The remainder of this paper is organized as in the following sections. Section 2 will describe the related works on mimicry attack in network. Section 3 will present the proposed ECC based data transmitting method. In Section 4, we will analyze the results of proposed method and compare it with standard methods. Finally, a brief conclusion will be given in Section 5.

II. RELATED WORK

C. Ateniese, *et al* was introduce a model for *provable data possession* (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage system. We present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation[13].

G. Ateniese *et al* stated that Proofs of storage (PoS) are interactive protocols allowing a client to verify that a server faithfully stores a file. Previous work has shown that proofs of storage can be constructed from any homomorphic linear authenticator (AUDITOR). The latter, roughly speaking, are signature/message authentication schemes where `tags' on multiple messages can be homomorphically combined to yield a `tag' on any linear combination of these messages. We provide a framework for building public-key AUDITORs from any identification protocol satisfying certain homomorphic properties. We then show how to turn any public-key AUDITOR into publicly-verifiable PoS with communication complexity independent of the file length and supporting an unbounded number of verifications. We illustrate the use of our transformations by applying them to a variant of an identification protocol by Shoup, thus obtaining the first unbounded-use PoS based on factoring (in the random oracle model)[14] .

B. Awerbuch *et al* stated that Ad hoc network and calculate the distance multihop communication model. This architecture makes services more vulnerable to internal attacks coming from compromised nodes that behave arbitrarily to disrupt the network, also referred to as Byzantine attacks. In this work, we examine the impact of several Byzantine attacks performed by individual or colluding attackers. We propose ODSBR, the first on-demand routing protocol for ad hoc wireless networks that provides resilience to Byzantine attacks caused by individual or colluding nodes. The protocol uses an adaptive probing technique that detects a malicious link after log n faults have occurred, where n is the length of the path. Problematic links are avoided by using a route discovery mechanism that relies on a new metric that captures adversarial behavior. Our protocol never partitions the network and bounds the amount of damage caused by attackers. We demonstrate through simulations ODSBR's effectiveness in mitigating Byzantine attacks. Our analysis of the impact of these attacks versus the adversary's effort gives insights into their relative strengths, their interaction, and their importance when designing multihop wireless routing protocols[15].

K. Balakrishnan, *et al* presented that Mobile ad hoc networks (MANETs) operate on the basic underlying assumption that all participating nodes fully collaborate in self-organizing functions. However, performing network functions consumes energy and other resources. Therefore, some network nodes may decide against cooperating with others. Providing these selfish nodes, also termed misbehaving nodes, with an incentive to cooperate has been an active research area recently. In this paper, we propose two network-layer acknowledgment-based schemes, termed the TWOACK and the S-TWOACK schemes, which can be simply added-on to any source routing protocol. The TWOACK scheme detects such misbehaving nodes, and then seeks to alleviate the problem by notifying the routing protocol to avoid them in future routes. Details of the two schemes and our evaluation results based on simulations are presented in this paper. We have found that, in a network where up to 40% of the nodes may be misbehaving, the TWOACK scheme results in 20% improvement in packet delivery ratio, with a reasonable additional routing overhead[16].

D. Boneh, *et al* portrays a short signature scheme based on the Computational Diffie–Hellman assumption on certain elliptic and hyper elliptic curves. For standard security parameters, the signature length is about half that of a DSA signature with a similar level of security. Our short signature scheme is designed for systems where signatures are typed in by a human or are sent over a low-bandwidth channel. We survey a number of properties of our signature scheme such as signature aggregation and batch verification [17].

III. PROPOSED WORK

The proposed method consists of five modules namely Network Configuration, Auditor, Setup Phase and Packet Transmission Phase, Audit Phase and Detection Phase and Performance Evaluation. The mimicry attack problem has been investigated using the traditional system. In our proposed scheme forward a two-factor authentication scheme based on ECC for prevention of various attack. Our new

scheme makes up for the missing security features necessary for real -life applications while inheriting the desired features of the original scheme. We prove that the scheme fulfills mutual authentication in the system. Moreover, by way of informal security analysis, we show that the new scheme can withstand various known attacks and provide more security features than existing scheme.

The architecture of the proposed work is given in the figure-1

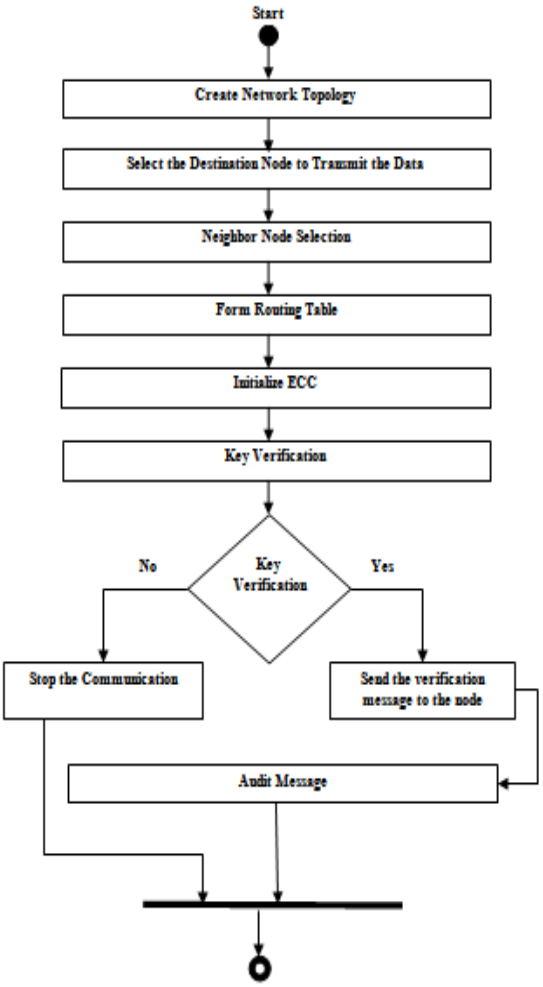

Figure-1 Proposed System Architecture

A. *Network Configuration*

In this paper mainly focus on static or quasi-static network. In wireless network our need to send the packet through the node. System is represented as a node. Here every node has communication range. By using this range only we can transmit over packet. If source and destination node exists within the communication range, source can directly transmit the packet. Otherwise, need to select the intermediate node based on the transmission range for transmit the packets.

B. *ECDSA Cryptography*

Elliptic Curve Digital Signature Algorithm is implemented over elliptic curve P-192 as mandated by ANSI X9.62 in C language. The Project contains necessary modules for domain parameters generation, key generation, signature generation, and signature verification over the elliptic curve. ECDSA has three phases, signature generation, key generation and signature verification.

- **Signature Generation**

To sign a message m, an entity A with domain parameters D= (q, FR, a, b, G, n, h) does the following:

1. Select a random or pseudorandom integer k in the interval [1, n-1].
2. Compute kP =x1, y1 and r= x1 mod n (where x1 is regarded as an integer between 0 and q-1). If r= 0 then go back to step 1.
3. Compute k -1mod n.
4. Compute s= k -1 {h (m)+dr} mod n, where h is the Secure Hash Algorithm (SHA-1). If s = 0, then go back to step 1.
5. The signature for the message m is the pair of integers (r, s).

- **Key Generation**

An entity A's key pair is associated with a particular set of EC domain parameters D= (q, FR, a, b, G, n, h). E is an elliptic curve defined over Fq , and P is a point of prime order n in E(Fq), q is a prime. Each entity A does the following:

1. Select a random integer d in the interval [1, n- 1].
2. Compute Q = dP.
3. A's public key is Q, A's private key is d.

- **Signature Verification**

To verify A's signature (r, s) on m, B obtains an authenticated copy of A's domain parameters D = (q, FR, a, b, G, n, h) and public key Q and do the following

1. Verify that r and s are integers in the interval [1, n-1].
2. Compute w = s -1mod n and h (m)
3. Compute u1 = h(m)w mod n and u2 = rw mod n.
4. Compute u1P + u2Q =(x0, y0) and v= x0 mod n.
5. Accept the signature if and only if v = r

B. Auditor

To correctly calculate the correlation between lost packets, it is critical to enforce a truthful packet-loss bitmap report by each node. The basic idea of our method is as follows. An Auditor scheme allows the source, which has knowledge of the Auditor secret key, to generate Auditor signatures $s_1, \ldots, s_M$ for M independent messages $r_1, \ldots, r_M$, respectively. The Auditor signatures are made in such a way that they can be used as the basis to construct a valid Auditor signature for any arbitrary linear combination of the messages, $\sum_{i=1}^{M} ciri$, without the use of the Auditor secret key, where *ci*'s are randomly chosen coefficients. A valid Auditor signature for $\sum_{i=1}^{M} ciri$, can be constructed by a node that does not have knowledge of the secret Auditor key if and only if the node has full knowledge of *s*1, . . . , *sM*. So, if a node with no knowledge of the Auditor secret key provides a valid signature for $\sum_{i=1}^{M} ciri$,, it implies that this node must have received all the signatures *s*1, . . . , *sM*.

C. *Setup Phase and Packet Transmission Phase*

This phase takes place right after route P_{SD} is established, but before any data packets are transmitted over the route. In this phase, S decides on a symmetric-key crypto-system (encrypt key, decrypt key) and K symmetric keys key1, . . . ,key_K, where encrypt key and decrypt key are the keyed encryption and decryption functions, respectively. S securely distributes decrypt key and a symmetric key $key_j$to node njon

PSD, for j = 1, . . . ,K. Key distribution may be based on the public-key crypto-system such as RSA: S encrypts key_j using the public key of node n_j and sends the cipher text to n_j. n_j decrypts the cipher text using its private key to obtain key_j.
After completing the setup phase, *S* enters the packet transmission phase. Before sending out a packet *Pi*, where *i* is a sequence number that uniquely identifies *Pi*, *S* computes *ri*= *H*1(*Pi*) and generates the Auditor signatures of *ri*for node *nj*, as follows

$sji= [H_2(i||j)u^{ri}]^x$, for j = 1, . . . ,K

where|| denotes concatenation. These signatures are then sent together with $P_i$to the route by using a one-way chained encryption that prevents an upstream node from deciphering the signatures intended for downstream nodes.

D. Audit Phase and Detecting Phase

This phase is triggered when the public auditor A_d receives an ADR message from S. The ADR message includes the id of the nodes on PSD, ordered in the downstream direction, i.e., n_1, . . . , n_K, S's Auditor public key information p_k= (v, g, u), the sequence numbers of the most recent M packets sent by S, and the sequence numbers of the subset of these M packets that were received by D. Recall that we assume the information sent by S and D is truthful, because detecting attacks is in their interest.

The public auditor A_d enters the detection phase after receiving and auditing the reply to its challenge from all nodes on P_{SD}. The main tasks of A_d in this phase include the following: detecting any overstatement of packet loss at each node, constructing a packet-loss bitmap for each hop, calculating the autocorrelation function for the packet loss on each hop, and deciding whether malicious behavior is present.

E. Performance Evaluation

In this module, evaluate the performance of simulation. Our using the xgraph for evaluates the performance. In this paper evaluate some performance metrics: Packet delivery ratio – the ratio of the total number of packets received by the destination node to the number of packet sent by the source, Packet loss – the total number of packet losses, during the data transmission, End-to-End delay – the time taken to be data transmitted from source node to destination node.

IV. PERFORMANCE EVALUATION

We simulated the energy efficient localization technique on Network Simulator (version 2.28) widely known as NS2, a scalable discrete-event driven simulation tool.

A. Simulation Model

The distributed coordination function (DCF) of IEEE 802.11 is used as the MAC layer in our experiments. It uses RTS and CTS packet. The values of the parameters used for simulation are as shown in Table1

TABLE 1: SIMULATION PARAMETERS

Parameters	**Values**
Topology Size	1000 m X 1000 m
No. of sensor nodes	30
MAC layer	IEEE 802.11
Simulation time	50 Secs
Traffic Source	Constant bit rate(CBR)
Node Placement	Random waypoint
Packet Size	512 bytes
Transmit Power	360 mW
Receive Power	390 mW
Idle Power	1 mW
Initial Energy	5.1 Joules
Transmission Range	500m
Routing Protocol	AODV
Speed	10m/sec

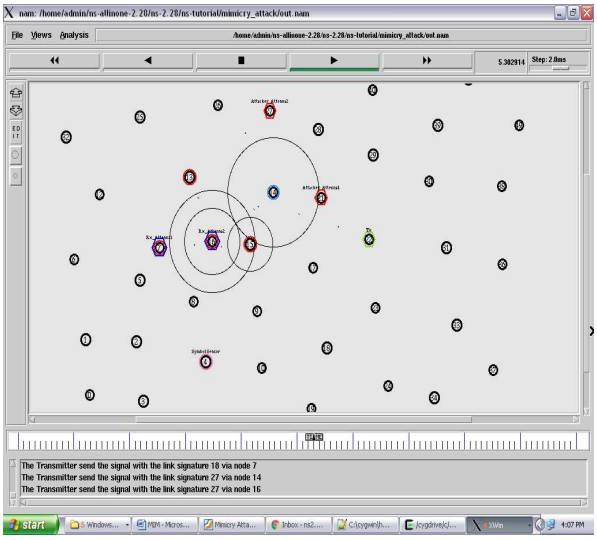

Figure-2 Link signature simulation

B. Results

The end-to-end delay is determined by calculating the average over all the surviving data packets from the source to the destination.

Figure-3 Delay difference between attacker and node

The link signature is determined by attacker and transmitter node.

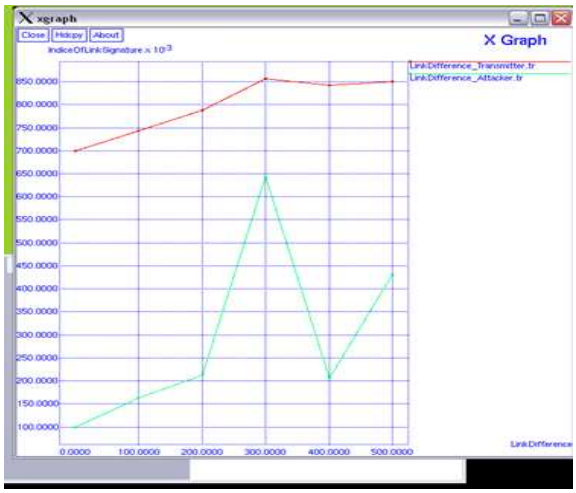

Figure-4 Link Difference between attacker and node

V. CONCLUSION

In this paper, we identified the mimicry attack against the existing wireless link signature schemes. We then extended the mimicry attack in MIMO systems and concluded that the attacker utilizing at least the same number of antennas as the receiver's antennas can successfully launch the mimicry attack. To defend against the mimicry attack, we proposed the time-synched link signature scheme by integrating cryptographic protection and time factor into wireless features. Our experimental results demonstrated both the feasibility of mimicry attacks and the effectiveness of the proposed method.

REFERENCES

[1] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signal prints," in Proc. ACM Workshop Wireless Secur. (WiSec), 2006, pp. 43–52.
[2] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures," in Proc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom), 2008, pp. 116–127.
[3] R. M. Gerdes, T. E. Daniels, M. Mina, and S. Russell, "Device identification via analog signal fingerprinting: A matched filter approach," in Proc. 13th Annu. Symp. Netw. Distributed Syst. Secur. (NDSS), 2006, pp. 1–11.
[4] L. C. C. Desmond, C. C. Yuan, T. C. Pheng, and R. S. Lee, "Identifying unique devices through wireless fingerprinting," in Proc. 1st ACM Conf. Wireless Netw. Secur. (WiSec), 2008, pp. 46–55.
[5] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in Proc. 13th Annu. ACM Int. Conf. Mobile Comput Netw. (MobiCom), 2007, pp. 111–122.
[6] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in Proc. 14th ACM Int. Conf. Mobile Comput. Netw. (MobiCom), 2008, pp. 26–37.
[7] 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.
[8] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in Proc. IEEE INFOCOM, Apr. 2013, pp. 3048–3056.
[9] 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.
[10] 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.
[11] 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.
[12] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca,"Ensemble: Cooperative proximity-based authentication," in Proc. 8th Int. Conf. Mobile Syst., Appl., Services (MobiSys), 2010, pp. 331–344.
[13] Ettus Research. The USRP Product Family Products and Daughter Boards, accessed on Apr. 2011.
[14] 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.
[16] R. Safaya. A Multipath Channel Estimation Algorithm Using a Kalman Filter, accessed on Apr. 2011. [Online]. Available: http://www.ittc.ku.edu/research/thesis/documents/rupul_safaya_thesis.pdf
[17] M. Biguesh and A. B. Gershman, "Training-based MIMO channel estimation: A study of estimator tradeoffs and optimal training signals," IEEE Trans. Signal Process., vol. 54, no. 3, pp. 884–893, Mar. 2006.
[18] K. S. Shanmugan and A. M. Breipohl, Random Signals: Detection, Estimation and Data Analysis. New York, NY, USA: Wiley, May 1988.
[19] O. Edfors, M. Sandell, J. J. van de Beek, S. K. Wilson, and
[20] P. O. Börjesson, "OFDM channel estimation by singular value decomposition "IEEE Trans. Commun., vol. 46, no. 7, pp. 931–939, Jul. 1998.