IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
21-23 September 2009, Rende (Cosenza), Italy

APEC - An Authentication Protocol with Embedded Certificates

Robert E. Hiromoto
University of Idaho, Moscow, Idaho 83844-1010, USA, hiromoto@uidaho.edu

***Abstract* - The APEC (Authentication Protocol with Embedded Certificates) is a wireless ad hoc network authentication protocol that employs a time-slots/frequency two-tuple for the validation of trusted nodes in a secure ad hoc network. APEC is derived from a canonical, time-space (frequency channel) splitting over which information (data packets) propagates under the constraint of a collision-avoidance protocol. In this paper, we analyze several authentication attack scenarios and discuss their properties under APEC.**

***Keywords* - Authentication, malicious attacks, space-time representation, time-slotted frequency-hopping spread spectrum.**

I. INTRODUCTION

The flexibility of wireless ad hoc networks is acknowledged as an important communication property in all aspects of homeland security and military communications. Unfortunately, the nature of such self-organizing networks is characterized by link failures, data packet collisions, and vulnerabilities from malicious attacks. Eavesdropping, man-in-the-middle, replay, impersonation, session hijacking, reflection, and interleaving categorize these attacks.

Numerous wireless network security protocols have been proposed by researchers in the establishment of secret key sequences and their application to certificate-based authentication of trusted nodes within a wireless ad hoc network. A taxonomy and classification of services that rely on authentication are studied by [1,2]. Authentication protocols using a local time-stamp [3], a hop-by-hop certification [4], a human behavior-inspired recommendation and referral scheme [5], location-limited channels with pre-authentication [6,7], an end-to-end data authentication scheme based on mutual trust between nodes [8] and threshold secret sharing [9], and loosely time synchronized nodes with a one-way cryptographic key chain with an associated time interval [10] have been proposed. [11] and [12] have looked at an alliance of trusted nodes formed with their immediate neighbors.

Recently, an alternative approach to certificate-based authentication has been proposed in [13]. In their proposed authentication protocol for wireless ad hoc networks with embedded certificates (APEC), they reformulate the authentication problem as a geometric splitting of time (time-slots) and space (frequency channels). Within this two-dimensional setting, a collision-avoidance policy is imposed on data transmission among wireless nodes that together removes the need for the explicit exchange of certificates in the authentication process.

In the remainder of the paper, we describe the APEC protocol, and illustrate its capabilities in protecting against selected malicious attacks.

II. BACKGROUND

The proposed APEC authentication protocol is a collision-avoidance, communication strategy that embeds authentication certificates as 2-tuples in a frequency/time-slot space. APEC introduces a sequence of unique, non-overlapping communication time-slots that are assigned to each authenticated node of the network. Time-slots provide collision-free communication links. In addition, each time-slot is assigned a pseudo-randomly correlated sequence of frequency channels $\{F_j\}_i$ (frequency-hopping spread spectrum) over which a data packet may be sent during time-slot T_i. This dependence between time-slots and frequency channels introduces a unique two-dimensional description of network communication, and allows for a 2-dimensional decomposition of the authentication domain.

A centralized server (cluster head) initializes the authentication phase by sending one or several public keys to all verified nodes in the network. Every node uses the public keys for the construction and selection of a pseudo-random number generator (PRNG), i.e., appropriate addem, multipliers; permutation matrices, and other predefined functions.

APEC employs at least two PRNGs, RandT() and RandF(), that produce sequences for T_i and F_i; respectively. Communication is now characterized as a space-time, 2-tuple coordinate basis, $(T_i, \{F_j\}_i)$. Time (time-slot), T_i, is taken as the moment (over the time-slot duration) that a message is sent or received. Space is the frequency channel, F_i, over which the message is sent or received.

Secure communication results by associating a $(T_i, \{F_j\}_i)$-tuple pair that uniquely defines a non-overlapping time ordering and a correlated frequency, known only within the wireless ad hoc network. Analogously, the uniqueness of the $(T_i, \{F_j\}_i)$ pair enforces a collision-avoidance or non-interfering communication policy. The collision-avoidance assumption restricts a clustered

network of wireless nodes to communicate only over predetermined, non-overlapping send or receive time-slots. The collision-avoidance assumption arises in the study of the QoS of unmanned aerial vehicles for autonomous formation flight [14]. As a consequence, certain types of external attacks can be detected if two or more distinct data packets arrive on different frequency channels during the same time-slot cycle. Thus each node realizes security and collision-avoidance properties by the deterministic coupling the communication time-slots to their assigned frequency channels. Figure 1 illustrates an *orthogonal* structure for a pair of PRNGs [15] that results in a reproducible pseudo-random number scheme for each node. This *orthogonal* structure was first developed to guarantee the reproducibility of results between a sequential (serial) Monte Carlo particle simulation to its corresponding parallel implementation. Using a node's ID and a public key, a random seed can be produced and used to seed RandT(). Each T_i generated is in turn used as a seed to generate a corresponding F_i from the pseudo-random number generator RandF().

APEC replaces the traditional certificate-based authentication procedures that have been proposed for infrastructure-less networks. The APEC approach can be summarized by the following set of properties: (1) a unique time-slot and frequency channel pair is assigned to each node within the network; (2) *conceals* the selection of the radio frequency channel F_i in each round of a node's communication time-slot sequence; (3) for each communication period a new sequence order for a given node's time-slots T_i may be assigned; and (4) the length of a time-slot duration depends upon the time-skewing experience by each node's clock (a GPS device for time synchronization is assumed for simplicity).

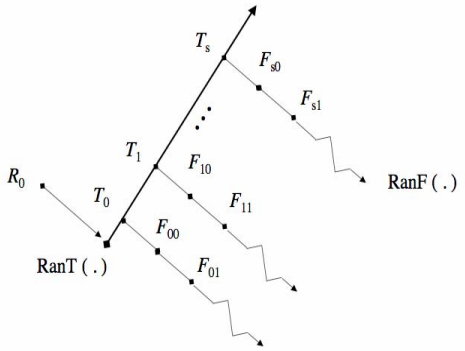

Fig. 1. RanT() and RanF().

Figure 2 illustrates a derivation of an APEC mapping scheme for a $(T_i, \{F_j\}_i)$-tuple space. The 3-dimensional abstraction indicates the role of RanF(T_i) as a third degree of freedom since many choices exist for the pseudo randomization process. This flexibility also increases the security aspects in discovering the correct sequence of frequency channels associated with each unique time-lot T_i. In addition, this flexibility allows for the use of chaotic systems in the construction of pseudo random sequences of the associated frequency channel. It should be noted that the pseudo random selection of time-slots represents a fourth degree of freedom, which is no shown in Figure 2.

III. ATTACK SCENARIOS

Four wireless network attacks are examined in this section. These types of attacks are (1) eavesdropping/jamming, (2) man-in-the-middle, (3) reflection, and (4) interleaving. These attack are normally difficult to defend against in a typical wireless ad hoc network.

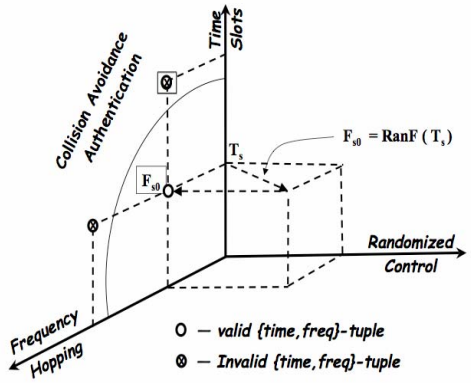

Fig. 2. APEC Mapping Scheme.

Eavesdropping and jamming are an intrusion with few self defense mechanisms provided by most wireless network security protocols. APEC takes advantage of the benefits of using spread-spectrum signals that provide a deterrent to deliberate jamming or to an eavesdropper, unless the pseudorandom sequence is known to the adversary. Frequency hopping by itself does not provide absolute protection against these two forms of attacks; however, the introduction of a unique communication time-slot and the use of encryption techniques can lead to mitigating potential weaknesses. Under a brute force attack of the pseudorandom sequence, the complexity of guessing the correct sequence would require an effort of

$$O(m \times 2^{2b}) \qquad (1)$$

where a *b*-bit pseudorandom sequence and *m* time-slots are assumed.

The man-in-the-middle (MITM) attack is a consequence of the physical limitations encountered between two communicating nodes that are beyond their radio range. In this scenario, a malicious agent attempts to gain the trust of a node (agent) that seeks a protected resource and a node that protects and controls access to the resource. This attack is a consequence of the hidden terminal problem where two nodes *A* and *B* are beyond each others radio range but within a mutual range of a (hidden) malicious node that acts to establish trust by

impersonating *A* to *B* and *B* to *A*. The MITM attack arises in both authenticated and non-authenticated protocols. An attack that may be viewed as a MITM is the interleaving attack that is discussed below. The analysis of the MITM attack is analogous to the eavesdropping attack. Here the malicious terminal must determine not only the pseudorandom sequences for node *A* but also for node *B*, which results in a complexity of $O(2^{2b+1})$, where the additional term in the exponent arises from setting $m = 2$ in equation (1).

A reflection attack attempts to trick a trusted node (the target) to reply to its own (authentication) challenge and, thereby, gain trusted channel access to the target. The following steps summarize the attack scenario (see Figure 3): (1) the attacker (dark filled circle) initiates a connection (dashed arrow over channel C_1) to a target (unfilled circle). (2) The target attempts to authenticate the attacker by sending it a challenge (solid arrow over the channel C_1 established by the attacker). (3) The attacker opens another connection (channel C_2) to the target, and sends the target this same challenge as its own. (4) The target responds to that challenge. (5) The attacker sends that response back to the target (i.e., *reflects it*) over the second connection. The APEC protocol, on the other hand, replaces the single challenge with a $(T_i, \{F_j\}_i)$-tuple pair that requires the attacker to gain knowledge of the entire sequences. The target in this case would either ignore the attacker's attempts in establishing channels C_1 and C_2 or report the observed attempts to a central security controller.

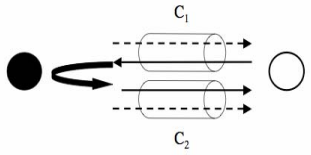

Fig. 3. Reflection Attack.

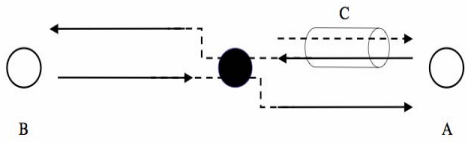

Fig. 4. Interleaving Attack.

An interleaving attack involves two trusted nodes *A* and *B* that know each other. An attacker tries to *bluff* one of the nodes by pretending to be the other node. This attack is similar to the MITM attack described above. The attack scenario is illustrated in Figure 4 and has the following steps: (1) The attacker establishes a connection (over channel C) with node *A*. (2) *A* challenges the attacker. (3) The attacker sends this challenge to *B*, the victim, who is led to believe that the challenge is sent by *A*. (4) The victim responds to this challenge. (5) The attacker forwards the same response to *A*. (6) *A* accepts the response and provides the services or information to the attacker. As in the case of MITM and the reflection attack, APEC treats the $(T_i, \{F_j\}_i)$-tuple pair as an embedded certificate scheme that requires detailed knowledge of the function sets employed.

The four or five attacks discussed here are difficult to mitigate in certificate-based authentication schemes. APEC provides a different perspective in addressing these attacks.

IV. Summary and Conclusion

APEC is an approach that formulates a two-dimensional description of communication within a wireless ad hoc network. A space-time splitting introduces a time-slotted, frequency correlated sequence as a coordinate basis in a $(T_i, \{F_j\}_i)$-tuple space.

We have presented several wireless network attacks that are difficult to prevent in current certificate-based authentication protocols. The collision-avoidance property of APEC and the correlated sequence of frequencies replace the static, certificate-based authentication tokens, with one that is both dynamic and difficult to guess.

The APEC presentation, however, has not addressed the issues of time synchronization and message encryption. One challenge facing frequency-hopping systems is the synchronization of the transmitter and receiver. This is currently under investigation but it is important to note that under APEC coordinated and *trusted* time synchronization can be performed between nodes. In the event that message or key encryption is required, protocols such as μTESLA [10, 16] may easily be incorporated within APEC.

References

[1] D. Park, C. Boyed, E. Dawson, "Classification of authentication protocols: a practical approach," *Proceedings of the Third International Workshop on Information Security*.

[2] S. Hahm, Y. Jung, S. Yi, Y. Song, I. Chong, and K. Lim, "Self-organized authentication architecture in mobile ad-hoc networks," *International Conference on Information Networking* (ICOIN) (2005).

[3] H. Lou, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing ad hoc wireless networks," *Seventh IEEE Symposium on Computers and Communications (ISCC'02)*.

[4] S. Zhu, S. Xu, S. Setia and S. Jajodia, "LHAP: A lightweight hop-by-hop authentication protocol for ad-hoc networks," *Proc. of ICDCS 2003 International Workshop on Mobile and Wireless Network (MWN 2003)*, May 2003.

[5] A. Weimerskirch and G. Thonet, "A Distributed light-weight authentication model for ad-hoc networks," *Proc. of 4th International Conference on Information Security and Cryptology (ICISC 2001)*.

[6] F. Stajano and R. Anderson, "The resurrecting duckling: security issues in ad-hoc wireless networks," M. Roe B. Christianson, B. Crispo, editor, *Security Protocols*, 7th International Workshop Proceedings, LectureNotes in Computer Science. Springer Verlag, 1999.

[7] D. Balfanz, D. K. Smetters, P. Stewart and H. Chi. Wong, "Talking to strangers: authentication in ad-hoc wireless networks," *Symposium on Network and Distributed Systems Security (NDSS '02)*.

[8] L. Venkatraman and D. Agrawal, "A Novel authentication scheme for ad hoc networks," *IEEE Wireless Communications and Networking Conference (WCNC 2000)*, vol. 3, pp. 1268-1273.

[9] H. Deng, A. Mukherjee, D. P. Agrawal, “Threshold and identity-based key management and authentication for wireless ad hoc networks," *International Conference on Information Technology: Coding and Computing (ITCC'04)*, 2004.

[10] S. Zhu, S. Setia and S. Jajodia, “LEAP: efficient security mechanisms for large-scale distributed sensor networks," *10th ACM Conference on Computer and Communications Security (CCS '03)*, 2003.

[11] Srdjan Capkun, Levente Buttyan, Jean-Pierre Hubaux, “Self-organized public-key management for mobile ad-hoc networks," in *ACM International Workshop on Wireless Security*, WiSe 2002.

[12] Chih-Peng Chang, Jen-Chiun Lin, Feipei Lai, “Trust-group-based authentication services for mobile ad-hoc networks," *1st International Symposium on Wireless Pervasive Computing*, 16-18 Jan. 2006.

[13] Robert E. Hiromoto and J. Hope Forsmann, “An authentication protocol for wireless ad hoc networks with embedded certificates," *Fourth International Workshop on Artificial Neural Networks and Intelligent Information Processing*, Funchal, Madeira - Portugal, May 14-15, 2008.

[14] J. Hope Forsmann, Robert E. Hiromoto, and John Svoboda, “A time-slotted on-demand routing protocol for mobile ad hoc unmanned vehicle systems," *SPIE 2007*, Orlando Florida, April 9-12 2007.

[15] P. Frederickson, R. Hiromoto, T. Jordan, B. Smith, and T. Warnock, “Pseudo-random trees in monte carlo," *Parallel Computing*, vol. 1, no. 2, pp. 175-180, (December 1984).

[16] A Perrig, R. Szewczyk, V. Wen, D. Culler, J.D. Tygar, “SPINS: security protocols for sensor networks," *Proc. of ACM Mobicom'01*, 2001.