Secure Multi-Hop Infrastructure Access

Baruch Awerbuch[1] Reza Curtmola[1] David Holmer[1] Cristina Nita-Rotaru[2] Herbert Rubens[1]

I. Introduction

Wireless networking today is predominantly used to provide mobile users with untethered access to fixed infrastructure. This allows users to move freely throughout the office or warehouse while remaining continuously connected with the office network and the Internet. While traditional access point devices currently provide this capability, they have a limited coverage range and thus many access points are required to provide coverage of a given area. One solution to this problem is to use a routing protocol that allows the users to traverse multiple hops to the nearest access point. This greatly expands the coverage range of each access point while simultaneously reducing costs and simplifying deployment.

Multi-hop infrastructure access has previously been proposed by [1] and [2]. However, the proposed solutions have only focused on routing without considering security. In this work we provide several extensions to the Pulse protocol [1] that defend against a large class of external attacks. The main contribution is providing strong adversarial resilience while maintaining low overhead.

The Pulse protocol was originally evaluated with an infrastructure only traffic pattern. Later work [3] evaluated the protocol under a more general mobile ad hoc network model with peer-to-peer traffic. The protocol was shown to achieve high delivery ratios under a wide range of network densities, mobilities, and traffic loads. The protocol operates with a periodic flood initiated by the infrastructure access gateway, which is referred to as the *pulse source*. This creates a proactively updated spanning tree throughout the network. The periodic pulse flood exploits the communication concentration at the pulse source by providing every node in the network with a continuously updated route. The proactive pulse flood provides scalability to high levels of mobility. As the mobility level increases, many failures begin to occur throughout the network. In the Pulse protocol, all broken routes are repaired simultaneously within one pulse interval using one flood. In contrast, an on-demand protocol may initiate one flood for every broken active route, and a proactive link-state protocol may generate one flood per link failure. As the number of failures increases, this results in congestion due to the additional routing overhead, limiting the scalability of these protocols to high levels of mobility.

While the performance and scalability of the protocol has been validated in existing studies, no existing work to our knowledge has addressed securing the protocol against adversarial attacks. In this work we present an efficient security framework for protecting the Pulse protocol operation from external adversarial attacks.

II. Problem Description

We consider an ad hoc network in which nodes obtain multi-hop access to fixed infrastructure (such as the wired network or Internet) by reaching the gateway (the pulse source).

We consider the following adversarial model: the gateway and all authenticated nodes are trusted to perform the routing protocol correctly. The adversaries are unauthenticated nodes that can perform arbitrary attacks (e.g. drop, inject or modify packets) and may collude to perform even stronger attacks (e.g. tunnel packets).

The protocol should offer a level of security comparable to state of the art single-hop protocols (e.g. 802.11i [4]). In addition, it has to offer protection against multi-hop routing attacks. Specifically, the routing protocol has to withstand the following attacks: packet injection, modification, replay, black holes, flood rushing, and wormholes. These are well-known attacks against wireless networks.

We assume that each node in the network has a unique pre-established shared secret (PSK) with the infrastructure access gateway, which is used for authentication. The PSK can be manually entered (as in WEP or WPA/WPA2 personal mode), or it can be automatically generated by an authentication server (as in 802.1x/EAP). The system must efficiently support adding and revoking nodes from the network.

III. Protocol Overview

We present a modified version of the Pulse protocol, which ensures packets are securely routed under the described adversarial model. In order to provide a secure routing service, all the nodes in the network share a network wide symmetric key (NSK). This key is used to provide packet authenticity and integrity. It is established and maintained using the key management scheme discussed below.

Our protocol establishes a reliability metric based on past history and uses it to select the best path. The metric is represented by link weights where high weights correspond to low reliability. Each node in the network monitors the performance of its links to its neighbors, and uses the resulting weights for selecting the shortest path. Faulty links are identified using secure acknowledgements on each link. Faulty links are avoided as their cost increases.

[1]Department of Computer Science, Johns Hopkins University, 3400 N. Charles St. Baltimore, MD 21218 USA. 410-516-5298 {baruch, crix, dholmer, herb}@cs.jhu.edu

[2]Department of Computer Science, Purdue University, 250 N. University Street, West Lafayette, IN 47907. 765-496-6757 crisn@cs.purdue.edu

IV. Protocol Operation

The protocol operates similarly to the original Pulse protocol, however all packets include a nonce for replay protection, and are encrypted and authenticated using the NSK. This prevents external adversaries from participating as nodes in the routing protocol. However, external adversaries can still execute several attacks against the protocol. For example, a pair of adversaries may create a wormhole, perform flood rushing on routing packets to increase the probability of being selected on a route, and then drop any drawn in data packet in a black hole attack. In order to protect against these types of attacks, a cryptographic acknowledgement is required for each data packet that traverses a link. This strategy is similar to the one used in ODSBR [5], however our adversarial model is different in that it excludes insider attacks. These acknowledgements allow the protocol to establish a secure loss-rate history for each link in the network. This secure loss-rate information is then used as a routing metric, similarly to ETX [6], which allows the protocol to select paths composed of reliable links.

V. Key Management

In this section we briefly describe some issues related to the management of keys in the system. All the participating nodes share a network wide symmetric key, NSK, which is used to provide packet authenticity and integrity.

While the set of participating nodes is dynamic, the network wide key NSK should be shared only by non-revoked nodes. Whenever nodes are revoked, the gateway needs to generate a new NSK and distribute it to the the set of valid nodes, so that revoked nodes are no longer able to participate in the protocol.

Since each node in the network has a pre-established individual shared key (PSK) with the gateway, the trivial solution would be for the gateway to unicast the new network key encrypted with the individual key to each node. However, this solution is inefficient. Instead, we use a broadcast encryption technique (e.g. LSD [7]), in which the gateway plays the role of the center. Specifically, we define the *join* and *revoke* operations for nodes:

- *join* - to join the network, a node communicates with the gateway using its individual PSK. Using this secure channel, the gateway provides the node with both the current network key NSK, and a number of subset keys. The subset keys are used by the broadcast encryption scheme, and will allow the node to decrypt updated versions of NSK in the future.
- *revocation & key refresh* - to update the network key, the gateway generates a new NSK, encrypts it using the broadcast encryption scheme, and floods it through the network. The broadcast encryption semantics ensure that revoked nodes will not be able to decrypt the new network key, even if they collude.

In the LSD broadcast encryption algorithm, the number of subset keys stored by each node is $O(log^{3/2}(n))$ (where n is the number of nodes in the network), the length of the broadcast message is $O(r)$ (where r is the number of revoked nodes), while each node will have to perform $O(log(n))$ inexpensive operations to decrypt the broadcast message. For example, even with 264 millon (2^{28}) potential nodes, the LSD scheme needs less than 3 kilobytes of storage per node (with 128-bit keys), and requires no more than 27 operations for any node to recover the key.

VI. Attack Analysis

Packet Injection or Modification: An HMAC with the NSK prevents an adversary from creating or tampering with valid packets.

Packet Replay: A nonce prevents an adversary from retransmitting previously transmitted packets on the network. The nonce is unique per node and replaced at every hop.

Black Hole: Black hole attacks are mitigated using the secure reliability metric to avoid unreliable links.

Wormhole: Wormhole creation is not prevented, however, the reliability metric allows nodes to avoid using wormhole links that do not deliver data packets.

Flood Rushing: The flood rushing attack exploits the timing sensitivity of routing protocols. Our protocol always prefers paths of lower metric regardless of timing, and is thus immune to flood rushing attacks.

VII. Conclusion

We presented a secure version of the Pulse Protocol for multi-hop infrastructure access. The protocol prevents a wide variety of external adversarial attacks. The protocol is light-weight and relies solely on symmetric cryptography.

References

[1] B. Awerbuch, D. Holmer, and H. Rubens, "The pulse protocol: Energy efficient infrastructure access," in *Proceedings of The 23rd Conference of the IEEE Communications Society INFOCOM*, 2004.

[2] S. Lee, S. Banerjee, and B. Bhattacharjee, "The case for a multi-hop wireless local area network," in *Proceedings of The 23rd Conference of the IEEE Communications Society INFOCOM*, March 2004.

[3] B. Awerbuch, D. Holmer, and H. Rubens, "The pulse protocol: Mobile ad hoc network performance evaluation," in *Wireless On-demand Network Systems and Services 2005*.

[4] *IEEE Std 802.11i-2004*. http://standards.ieee.org/getieee802/802.11.html.

[5] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An on-demand secure routing protocol resilient to byzantine failures," in *ACM Workshop on Wireless Security (WiSe) 2002*, 2002.

[6] D. S. J. D. Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless networks," in *9th annual international conference on mobile computing and networking (MobiCom 03)*, September 2003.

[7] D. Halevy and A. Shamir, "The LSD broadcast encryption scheme," in *Advances of Cryptology - Crypto '02*, vol. 2442 of *LNCS*, pp. 47–60, Springer-Verlag, 2002.