This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2006 proceedings.

Secure Ad Hoc Networking

Panagiotis Papadimitratos
Virginia Polytechnic Institute and State University
papadp@vt.edu

Abstract

The ad hoc networking technology can enable novel civilian and military applications. However, ad hoc networking protocols are vulnerable to a wide range of attacks. The design of defense mechanisms is a challenging problem, especially in comparison to securing traditional, fixed-infrastructure networks. In this paper, we discuss challenges and guidelines to secure ad hoc networking protocols, and describe a protocol suite for secure and fault-tolerant communication.

1. Introduction

Our perception of the Internet and network access habits have changed significantly over the last few years, with 60 million laptop computers in the US, 70% of the 45 million business travelers carrying a laptop, and 15 million users working on the road daily. 20 million computers will be wireless enabled by 2006, and wireless broadband Internet access will be available in 150 thousand locations worldwide, from a mere 1200 locations back in 2001. At the same time, an increasing number of community wireless networks, interconnecting desktop computers and routers throughout neighborhoods, are being deployed. Furthermore, most portable digital assistants and palmtop computers are now equipped with radio and infrared transceivers, while cellular telephones offer alternative ways of data communication. Overall, the network itself undergoes a gradual transformation.

The emerging *Mobile Ad hoc Networking* (*MANET*) technology will play a central role, enabling devices to communicate across multiple wireless links (hops) and areas larger than their transceiver range. Most important, a fixed networking infrastructure will not be necessary. Instead, network entities will collaborate to support basic networking operations, i.e., routing and data forwarding, and make up for the absent infrastructure.

Ad hoc networks may be formed in an impromptu manner: conferees exchanging information or forming workgroups, car computers disseminating warnings to avoid traffic jams, downloading maps or traveler's guides from 'info-kiosks,' home computers and wireless routers forming mesh networks. Ad hoc networks may also be deployed on-demand: in disaster relief scenarios, consisting of firefighters, policemen, medical personnel, and robots, or in battlefields, comprising military vehicles, aircrafts, and personnel. They may operate autonomously, or extend the fixed infrastructure, allowing, for example, remote wireless access points or alternate base stations to be reached across multi-hop paths.

The assumption underlying the development of ad hoc networking protocols has been that entities participate voluntarily and assist the network operation. However, assuming a benign environment is utopian, as experience from the development of the (wire-line) Internet teaches us. Numerous documented incidents and outages showed that the network and the interconnected systems are vulnerable to a wide range of attacks. This is emphatically so in the open and volatile ad hoc networking environment. Unlike traditional networks, the self-organizing ad hoc networking infrastructures are not well protected, closely monitored, and managed, and practically any network entity can become part of the infrastructure.

The challenge lies exactly in securing the ad hoc network operation, because any malicious or selfish network entity can disrupt, degrade, or even deny communication of other entities. Securing the network operation is paramount for both civilian and tactical applications. Users would have no incentive to embrace new products if, for example, they cannot access their services and get the quality they paid for, if the available resources are monopolized by adversarial nodes, or if their privacy is at stake. Similarly, a General or a Police Commissioner would not endorse networking technologies that do not guarantee secure and reliable communications in a battlefield or an emergency situation.

In this paper, we discuss the design of secure ad hoc networking protocols, providing a system model, identifying challenges and guidelines, and describing a secure and fault-tolerant communication protocol suite for ad hoc networks.

1-4244-0086-4/06/$20.00 ©2006 IEEE.

2. System Model

Mobile hosts collaboratively support the ad hoc network operation without necessarily pursuing a common objective or running the same application. The network membership and connectivity change frequently, as nodes may join and leave the network without prior notice, e.g., due to mobility or because devices alternate between 'sleep' and 'active' periods. As a result, the definition of the network area may change constantly, to include access points and services reachable by the freely migrating hosts, while there may be no administrative boundaries.

It is often implied that a network node is a host equipped with a wireless network interface. However, hosts may have more than one network interface, while the interface identifier, whether the hardware address or the *IP* address, can be easily changed in most platforms. We define a network *node* as a process with (*i*) a unique identity V, (*ii*) a public/private key pair E_V, D_V, (*iii*) a module implementing the networking protocols, as those defined in this dissertation, and (*iv*) a module providing communication across a wireless network interface.

In this work, we focus on the network operation above the data-link layer, with transmissions over a broadcast radio channel, such as the *IEEE 802.11*. We are concerned with pair-wise communication across multiple wireless links between a *source, S,* and a *destination, T*. We denote S and T as the *end nodes*, and nodes that assist the *S, T* communication as *intermediate nodes.*

We assume that nodes can obtain keying material for other nodes in the network; in particular, that each end-node knows the identity and the public key of its peer end-node, and all nodes know the identities and the public keys of their neighbors, unless noted otherwise. The possession of keys does not imply authorization, but it is a minimum requirement for each node to engage in secure communication.

Ad hoc nodes in physical proximity can establish keying material through local off-line channels. In general, however, key certification will be necessary, to ensure a one-to-one relationship between node identities and credentials. The exchange of keying material can be integrated into the neighbor discovery or an initial route discovery. The validation of certificates will be possible either through *Certification Authorities* (*CA*s), or trust chains comprising certificates generated by other users. A number of approaches are proposed in the literature; due to space limitations, we refer the reader to the discussion in [1-2].

Nodes may be *correct*, i.e., fully comply with the networking protocols, or *faulty*, i.e., deviate from the protocols' definition. Faulty nodes may exhibit malicious behavior, in which case we say that those nodes are *adversaries*. They can disrupt or abuse the operation of any of the networking protocols, corrupting, discarding, forging, and replaying data and control traffic. Formal discussion and definition of the adversary model is given in [1].

3. Challenges and Guidelines

Nodes are assisted by other nodes without any prior association, as, in general, they communicate across largely unknown networks. As a result, they do not possess the credentials of all other nodes, this being especially true for large-scale ad hoc networks.[1]

Nodes lack in general the means to classify their peers as trustworthy or adversarial. Pre-configuring nodes with such knowledge is clearly hard for an open, civilian network with disparate, transiently associated nodes. But it can be hard in a tactical network, where initially trusted nodes can be hijacked.

The possession of credentials cannot guarantee that a node is correct. Virtually any node in the network can disrupt or abuse the protocol operation, and degrade or deny the communication of any other node in the network.

Distinguishing malicious faults from network impairments is hard. For example, can packet loss due to mobility-induced or medium access contention link breakages be distinguished from the case that the relaying node discards the packet? This problem becomes harder when adversaries disguise their misbehavior as benign faults.

Finally, systems enabled by ad hoc networks will operate under a multitude of environmental constraints and application requirements. A single protocol that outperforms all alternative ones in all settings may not exist. To address the above-mentioned challenges, a comprehensive security solution that can operate in a variety of network conditions is necessary.

First, a secure routing protocol to safeguard the discovery of communication paths is needed. It must prevent adversaries from influencing, controlling, or abusing the route discovery, e.g., by impersonating network destinations, advertising unreachable destinations or links not reflecting factual connectivity, or misleading their peers that a destination can be reached at a lower (higher) cost than the actual one must be prevented. A *specification*, i.e., a definition of the sought properties of the routing protocol in the presence of adversaries, independently of how the protocol operates, is provided in [1]. We say that a

[1] Closed, mission-specific tactical networks are an exception, but, clearly, generalizing such an assumption would significantly narrow the scope of ad hoc networking.

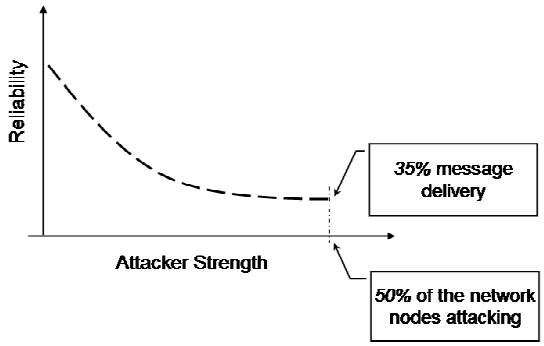


Figure 1. Communication with security only for the route discovery.

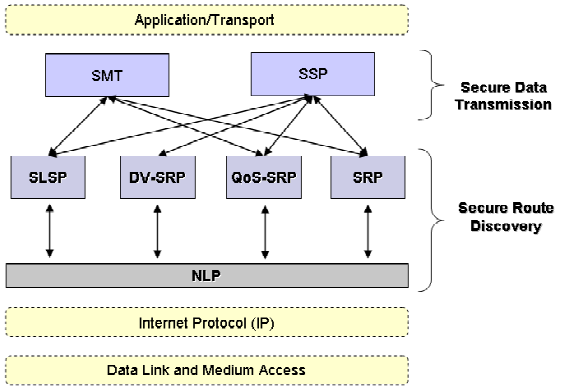


Figure 2. Secure Communication Protocol Suite.

discovered route is *correct* if it satisfies the specification.

Nevertheless, correct routes are not guaranteed to be adversary-free. A secure routing protocol cannot detect an intelligent adversary that fully abides with the route discovery, and only later, once it becomes part of a utilized route, disrupts the data communication. Fig. 1 illustrates the impact of such an adversary when security is provided only for the route discovery [3]: the reliability of communication drops fast as the fraction of adversarial nodes present in the network increases. Thus, securing both phases of communication, the route discovery and the data transmission, is paramount.

Security services (data authenticity and integrity, and replay protection) along with robust detection of communication faults are necessary to secure the data transmission. Data loss must be detected, so that corrective actions are taken, i.e., non-operational or compromised routes are avoided, and lost data are re-transmitted across operational routes. Clearly, the fault detection scheme must thwart intelligent adversaries that attempt to hide their presence and continue disrupting communication across routes they control.

Designing a secure data transmission protocol that relies only on end-to-end security bindings is a particularly attractive choice. End-to-end operation can eliminate abuse of the route maintenance operation, alleviate the need of prolonged observation periods to characterize misbehaving nodes as adversaries, avoid the vulnerability to 'blackmail' attacks by adversaries disseminating false misbehavior reports, and the overhead and the resultant delay of message exchanges with all nodes along a faulty route.

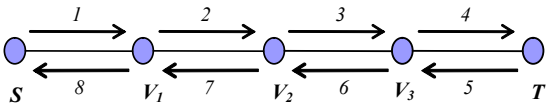
4. A Secure Communication Protocol Suite

We designed a protocol suite to secure the basic networking operation, that is, the route discovery and the data forwarding, and achieve our primary goal, the availability of communication across frequently changing, unknown networks in the presence of adversaries. The protocol suite is shown in Fig. 2. The data transmission phase is secured by the *Secure Message Transmission (SMT)* and *Secure Single Path (SSP)* protocols [3-4], which rely on an underlying secure routing protocol: the *Secure Routing Protocol* (*SRP*) [5], the *Quality-of-Service* aware *QoS-SRP* [6], the *Distance-Vector DV-SRP* [7], and the *Secure Link State Protocol* (*SLSP*) [8], which interoperate a secure neighbor discovery protocol, the *Neighbor Lookup Protocol* (*NLP*) [1]. Protocols from each category can be combined, even though specific combinations, such as *SRP* combined with *SMT* for example, are more versatile and effective.

NLP provides localized neighbor discovery and traffic authentication, with nodes exchanging keys and certificates, and establishing shared keys. Equally important, *NLP* prevents adversaries from utilizing multiple identities. Protocols bounding the propagation delay and thus the data link transmission distance (e.g. [9]) can prevent adversaries from acting as raw data (signal) repeaters. Since these protocols necessitate authentication of transmissions between neighboring nodes, the two tasks should be naturally combined.

SRP is a reactive routing protocol suitable for a broad range of *MANET*s, operating in an end-to-end manner without restrictive assumptions on network trust and security associations. Low route discovery delay with low network and processing overhead can be achieved, even when a significant fraction of the network nodes disrupt the route discovery. The operation of *SRP* is illustrated in Fig. 3, with Q_{ID}, Q_{SEQ} identifiers of the *RREQ*, $K_{S,T}$ a symmetric key shared by *S*, *T*, and *MAC* a message authentication code.

QoS-SRP thwarts adversaries that manipulate link and route metrics to influence the route selection. It



Route Request (*RREQ*): $S, T, Q_{SEQ}, Q_{ID}, MAC(K_{S,T}, S, T, Q_{SEQ}, Q_{ID})$
(1) S broadcasts *RREQ*;
(2) V_1 broadcasts *RREQ*, V_1;
(3) V_2 broadcasts *RREQ*, V_1, V_2;
(4) V_3 broadcasts *RREQ*, V_1, V_2, V_3;

Route Reply (*RREP*): $Q_{ID}, T, V_3, V_2, V_1, S,$
$MAC(K_{S,T}, Q_{ID}, Q_{SEQ}, T, V_3, V_2, V_1, S)$

(5) $T \rightarrow V_3$: *RREP*;
(6) $V_3 \rightarrow V_2$: *RREP*;
(7) $V_2 \rightarrow V_1$: *RREP*;
(8) $V_1 \rightarrow S$: *RREP*;

Figure 3. *SRP* operation.

enables *QoS*-aware routing by ensuring that the quantitative description (i.e., the attributes) of the discovered routes is reasonably close to their actual metric values. The basic difference of *QoS-SRP* from basic *SRP* is the accumulation of link metrics in the control packets, and a set of processing steps at end and intermediate nodes. The route metric is the aggregate of the link metrics. A wide range of link route metrics are supported. With explicit information on each individual link, *QoS-SRP* can support any route calculation algorithms at the source node.

DV-SRP discovers on-demand routes, establishing them across the network without providing explicitly the network connectivity. *DV-SRP* combines the advantages of the Ad hoc On-Demand Distance Vector type of route discovery with security and thus resilience. It prevents adversaries from manipulating the length (hop count) of the discovered routes, uses primarily symmetric key and thus low cost cryptographic primitives, and can discover multiple routes. However, the fundamental difference of secure distance vector protocols such as *DV-SRP* from *SRP* and *QoS-SRP* lies in the requirement to authenticate the origin of *RREQ* and *RREP* (i.e., end nodes) at intermediate nodes. Nevertheless, *DV-SRP* can perform this task efficiently, with the intermediate nodes verifying the origin authenticity of the control packets.

SLSP is a (proactive) protocol for discovery and distribution of link state information, with nodes information for their *R*-hop neighborhood or zone, as illustrated in Fig. 4. Signed *link state update* (*LSU*) packets are broadcasted, with receiving nodes validating the *LSU*s, suppressing duplicates, and relay packet that did not already propagate *R* hops. Link state acquired from validated *LSU*s is accepted only if it is advertised by both nodes incident on the link. *SLSP* provides for each node to distribute its public

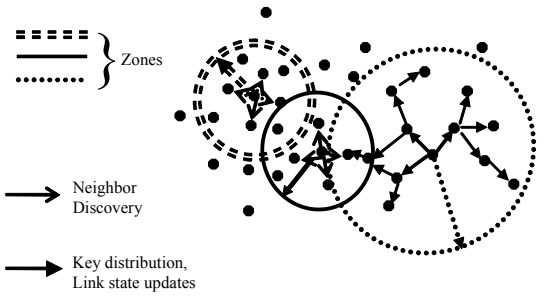


Figure 4. *SLSP* operation.

key to nodes within its zone, either by *Public Key Distribution* (*PKD*) packets, or by attaching the keys to *LSU* packets. As the network topology changes, nodes learn the keys of nodes that move into their zone; *PKD* packets may distribute keys less frequently throughout an extended zone ($R'>R$), to reduce the delay of validating new keys when nodes eventually enter the zone. The propagation of *LSU* or *PKD* within R (or R') hops is loosely enforced.

SMT and *SSP* operate without restrictive assumptions on the network trust and security associations, promptly detect and avoid non-operational or compromised routes, tolerate loss of data and control information, and adapt to the network conditions. Their main difference is that *SMT* utilizes multiple paths simultaneously, in contrast to *SSP*'s the single path operation.

In Fig. 5, *S* disperses the message so that any three out of the four transmitted pieces are sufficient for successful reconstruction of the original message. Two of the pieces, each routed across a different route, arrive intact at the receiver, while the remaining two pieces are compromised by adversaries on the transmission paths; e.g., one piece is dropped and one (dashed arrow) is modified. The cryptographic integrity check reveals the corrupted data, *T* rejects the piece and waits for additional message pieces (as determined in the header of incoming validated pieces), after setting a reception timer. At the timer expiration, the destination feedback is returned across

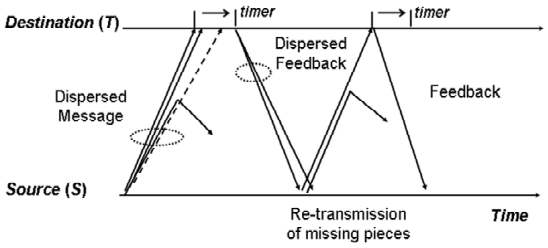


Figure 5. *SMT* message transmission example.

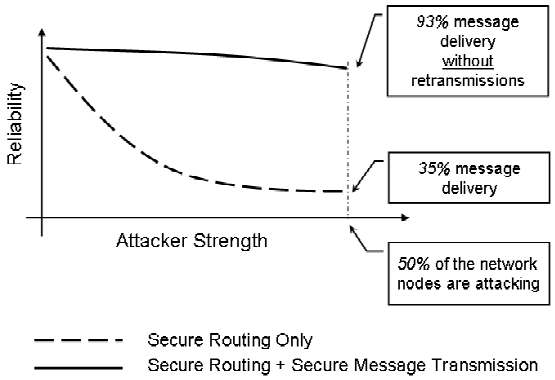


Figure 6. Securing both the data transmission and the route discovery, compared to secure routing only.

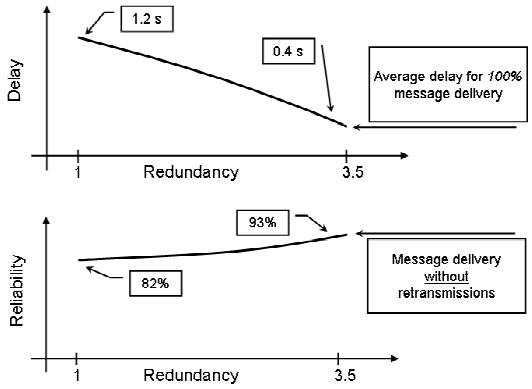


Figure 7. Secure data communication: adaptation to the network conditions and application requirements.

the two operational paths. The sender receives and validates the feedback, ignoring duplicates, and retransmits the two missing pieces. One of them is lost, for example, because of intermittent malicious behavior, however, the destination has an adequate number of packets (3 out of 4), and acknowledges the successful reception to complete the message transmission.

Integrating *SMT* and *SSP* with secure routing reveals the importance of securing both phases of communication. In Fig. 6, *SMT* delivers 93% of transmitted messages even when 50% of the network nodes disrupt the data transmission [4]. More important, highly reliable communication is achieved without retransmissions. As a result, *SMT* can support time-sensitive or real-time communication even in highly adverse settings, with near-constant delay and delay jitter.

This is achieved with moderate network overhead, with *SMT* configuring transmissions to either achieve strong protection, or efficient operation. In the extreme case, *SSP* eliminates multipath transmission overhead. Highly reliable communication is achieved while sacrificing the real-time aspect, trading off delay for overhead. Fig. 7 shows the versatility of *SMT/SSP* which can be highly effective even in resource constrained environment, and overall achieve strong protection and be practical.

6. Conclusions

The secure communication protocol suite discussed in this paper can be widely applicable, being both effective, achieving highly reliable, low-delay and low-jitter communication even in highly adverse settings, and, at the same time, capable to operate in resource-constrained settings. However, our solution is not exhaustive, as there exists a range of additional security aspects largely orthogonal to denial of service, such as key and trust management, anonymity, and privacy.

7. References

[1] P. Papadimitratos, "Secure and Fault-Tolerant Communication in Mobile Ad Hoc Networks," *PhD Dissertation*, Cornell University, January 2005

[2] P. Papadimitratos and Z.J. Haas, "Secure Communication in Adverse Mobile Ad Hoc Networks," *Ad Hoc Wireless Networking*, D-Z. Du, Ed., Kluwer Academic Publishers, MA, November 2003

[3] P. Papadimitratos and Z.J. Haas, "Secure Message Transmission in Mobile Ad Hoc Networks," in Proc. of the *ACM WiSe 2003,* San Diego CA, Sept. 2003

[4] P. Papadimitratos and Z.J. Haas, "Secure Data Communication in Ad Hoc Networks," *IEEE Journal on Selected Areas in Communication,*2nd quarter, 2006 (*to appear*)

[5] P. Papadimitratos and Z.J. Haas, "Secure Routing for Mobile Ad Hoc Networks," in Proc. of the *CNDS 2002*, San Antonio, TX, Jan. 27-31, 2002

[6] P. Papadimitratos and Z.J. Haas, "Secure QoS-aware Route Discovery in Ad Hoc Networks," in Proc. of the *2005 IEEE Sarnoff Symposium*, Princeton, NJ, Apr. 2005

[7] P. Papadimitratos and Z. J. Haas. "Secure On-Demand Distance-Vector Routing in Ad Hoc Networks." In Proc. of the *2005 IEEE Sarnoff Symposium*, Princeton, NJ, Apr. 2005

[8] P. Papadimitratos and Z.J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks," in Proc. of the *IEEE CS Workshop on Security and Assurance in Ad hoc Networks*, Orlando, FL, Jan. 2003

[9] S. Brands and D. Chaum, "Distance-bounding protocols (extended abstract)," *In Theory and Application of Cryptographic Techniques*, p. 344–359, 1993