Handling New Adversaries in Secure Mobile Ad-hoc Networks

Virgil D. Gligor
Electrical and Computer Engineering Department
University of Maryland
College Park, Maryland 20742

1. The Problem

Invariably, new technologies introduce new vulnerabilities which often enable new attacks by increasingly potent adversaries. Yet new systems are more adept at handling well-known attacks by old adversaries than anticipating new ones. Our adversary models seem to be perpetually out of date: often they do not capture adversary attacks and sometimes they address attacks rendered impractical by new technologies. An immediate consequence of using an out-of-date adversary model with a new technology is that security analysis methods and tools cannot possibly handle the new vulnerabilities thereby leaving users exposed to new attacks. An equally compelling reason for investigating new adversarial capabilities in Mobile Ad-hoc Networks (MANETS) is this: without a precise adversary definition the very notion of security becomes undefined. For instance, the fundamental question of "what is the set of threats addressed" by a given secure protocol cannot be answered without an adversary definition.

In short, we need to provide (1) a new definition for the new adversary attacks made possible by Mobile Ad-hoc Networks (MANETS), (2) demonstrate that this new definition is more general than the traditional, formal network adversary models (including the classic Dolev-Yao and Byzantine models), (3) illustrate how this new adversary is countered with new practical protocols that operate under realistic performance and cost constraints. Interesting protocols to investigate using the new adversarial definition include those typically used in MANET management, distributed sensing and data fusion, as well as the more traditional authentication protocols for principal and node-to-node authentication.

2. Background

A common vulnerability of MANETS, and in general of all networks whose nodes operate in hostile environments, is is the possibility of physical capture and control of network devices by an adversary. Frank Stajano's "big stick principle," which states that whoever has physical control of a device is allowed to take it over, suggests that such an adversary is "difficult" to counter. In fact, no amount of device protection, nor increased computational workload imposed on this adversary, seems to suffice: the adversary can selectively control the inputs to network devices without causing physical tampering and thus can corrupt network operations, and can selectively jam the outputs of network devices in a stealthy manner and thus deny network operations. This implies that protecting device secrets (e.g., cryptographic keys) via physical security measures, which currently range from those employed by smartcards (very little tamper resistance) to those of IBM 4758 crypto co-processors (highest FIPS 140 evaluation), is both unrealistic and inadequate in the face of the new adversary. Even when the cost of strong physical security measures is affordable in some traditional networking environments (e.g., banking), such protection is inadequate in MANETS because access to a node's internal state is (1) usually possible without direct access to the protected cryptographic keys and (2) typically the form factors and resource requirements (e.g., energy) of the protective devices (e.g., IBM 4758 card) are not suitable for the limited power and small form-factor MANET nodes. Thus, in captured MANET nodes (e.g., PDAs, laptops) access to the internal states by an adversary cannot always be prevented.

A further problem caused by this new and "difficult" adversary is that of adaptive capture of MANET nodes: once a node is physically captured and its internal state discovered, all the secrets (e.g., cryptographic keys) which the node may use for authentication with with other nodes are compromised. Now the adversary can proceed to selectively capture additional nodes that execute network applications. Thus the new adversary can control multiple nodes of a network thereby enabling *collusion attacks* perpetrated by cooperating captured nodes.

A new MANET adversary model should include new features that are currently not present in the traditional formal models. To see this, let us recall, for instance, the key features of the Dolev-Yao model that dominated most analysis of cryptographic protocols for the past two decades. The Dolev-Yao model has three basic components, namely:

1) the presence of the the "man-in-the-middle" (MITM) everywhere in the network. That is, the adversary can launch any MITM attack on any and all network links and thus can read, replay, block, insert messages anywhere.

2) the adversary can send and receive messages from any legitimate principal (e.g., node) of the network. Thus, the adversary can freely communicate with all legitimate principals and nodes of the network and use them as oracles in attempts to discover secrets and forge messages. And,

(3) the adversary can be a legitimately registered principal of the network. Thus, s/he can attack other network nodes by exploiting protocol features and vulnerabilities.

While the Dolev-Yao adversaries appear to be extremely powerful in any network, they lack the capabilities of the new network adversary enabled by MANETS. For instance, the Dolev-Yao adversary cannot capture network nodes an discover other principals' or other nodes' secrets. Further, this adversary does not address the threat of *collusion attacks* launched by cooperating captured nodes under the adversary's control. Finally, this adversary cannot modify a network's trust and physical topology. For instance, a Dolev-Yao adversary cannot read a node's internal state, replicate it on other nodes under its control and insert the controled nodes within the network.

A similar analysis shows that the traditional Byzantine adversaries typically used in consensus protocols are also less general than the new MANET adversaries. For example, such adversaries have a "threshold" behavior: below a fixed threshold of captured nodes they can be countered (e.g., 1/3 captured nodes if message authentication cannot be provided and a simple minority, otherwise). In MANETS applications, substantial damage can be perpetrated even by capturing substantially fewer nodes than the Byzantine thresholds indicate. Further, the traditional notion of adversary "mobility," which suggests that the Byzantine adversary captures a set of up to "t" nodes in some protocol state and then captures a totally different set of up to "t" nodes in another state [5], has changed. The new adversary's behaviour is monotonic and not limited to "t" nodes: once a node is captured, it stays that way and the number of captured nodes is not limited to a fixed threshold value, "t."

3. What is Needed ?

We suggest that an adversary model is needed that is suitable for the new threats posed by using MANET technologies in hostile environments. Once a comprehensive definition of the adversary is given, it become necessary to investigate how this adversary can be handled in practical ways within the preformance and cost constraints of typical MANETS. Specifically we nned to investigate how to handle the new adversary within specific MANET protocols.

While perfect physical security of ad-hoc network devices is both currently unrealistic and fundamentally inadequate a goal, "good-enough" network security in the face of "difficult" MANET adversaries can be obtained with relatively inexpensive technologies. For example, algorithmic adversary-detection technologies can be based on *emergent properties and protocols*. Intuitively, emergent properties are features that cannot be provided by individual network nodes themselves but instead result from interaction and collaboration among these nodes. Although one may think of the creation of an ad-hoc network as a set of emergent connectivity and routing properties, our primary focus is on the specific properties that may emerge after the ad-hoc networks are thus established. The emergent properties and protocols we propose to study for the handling of "difficult" MANET adversaries are different from traditional network properties established via protocol interactions in several fundamental ways. First, it is possible that neither the time nor the locus of emergence of these properties can be easily anticipated. Second, the emergence of these properties may be uncertain, in the sense that it may be probabilistic. Third, these properties may be transient, in the sense that they may disappear from the ad-hoc network during normal operation and not as a result of exceptional events; e.g., node or protocol failures.

We believe emergent properties and protocols are essential to handling "difficult" adversaries; e.g., adversaries that exceed the powers of the traditional "Dolev-Yao" and "Byzantine" adversaries. Emergent properties can be used to detect, often probabilistically, the presence of a "difficult" adversary and to pinpoint with reasonable accuracy the affected network area (e.g., identify a specific captured node, a particular property of captured nodes) [6, 4]. Correct assessment of node capture and replication is important for otherwise false detection may also lead to node revocation [2], which in turn may lead to network partitioning and denial of service. Similarly missed detection may lead to node replication and collusion among replicas also leading to network partitioning and/or false data injection and application corruption.

Finally, emergent properties help determine the scalability and resilience of ad-hoc networks. For example, emergent properties (such as establishment of secure communication paths in sensor networks via random key pre-distribution) may place constraints on the network size but may also imply resilience of network communications below a certain threshold of compromised nodes [1].

References

[1] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. of the IEEE Security and Privacy Symposium, Berkeley, CA, May 2003 (available at *http://www.ece.cmu.edu/~adrian*).

[2] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, "On the Distribution and Revocation of Cryptographic Keys in Sensor Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 3, July-Sept. 2005.

[3] L. Eschenauer, V.D Gligor, and J.S. Baras, "On Trust Establishment in Mobile Ad-Hoc Networks", in *Security Protocols*, Christianson *et al.* (eds.), Cambridge, UK, April 2002. (available at *http://www.ee.umd.edu/~gligor*)

[4] J. McCune, E. Shi, A. Perrig and M. K. Reiter. "Detection of Denial-of-Message Attacks on Sensor Network Broadcasts," Proc. of the IEEE Symp. on Security and Privacy, Oakland, California 2005

[5] R. Ostrovsky and M. Yung, "How to Withstand Mobile Virus Attacks," ACM Symp. on Principles of Distributed Computing, 1991, pp. 51-59.

[6] B. Parno, A. Perrig, V. Gligor "Distributed Detection of Node Replication Attacks in Sensor Networks," IEEE Symposium on Security and Privacy, Oakland, CA. 2005. (available at *http://www.ece.cmu.edu/~adrian*).