

Adaptive Security for Multi-layer Ad-hoc Networks

Jiejun Kong, Haiyun Luo, Kaixin Xu, Daniel Lihui Gu, Mario Gerla, Songwu Lu
UCLA Computer Science Department
{jkong,hluo,xkx,gu,gerla,slu}@cs.ucla.edu

Abstract

Secure communication is critical in military environments where the network infrastructure is vulnerable to various attacks and compromises. A conventional centralized solution breaks down when the security servers are destroyed by the enemies. In this paper we design and evaluate a security framework for multi-layer ad-hoc wireless networks with unmanned aerial vehicles (UAVs). In battlefields, the framework adapts to the contingent damages on the network infrastructure.

Depending on the availability of the network infrastructure, our design is composed of two modes. In *infrastructure mode*, security services, specifically the authentication services, are implemented on UAVs that feature low overhead and flexible managements. When the UAVs fail or are destroyed, our system seamlessly switches to *infrastructureless mode*, a backup mechanism that maintains comparable security services among the surviving units. In the *infrastructureless mode*, the security services are localized to each node's vicinity to comply with the ad-hoc communication mechanism in the scenario. We study the instantiation of these two modes and the transitions between them. Our implementation and simulation measurements confirm the effectiveness of our design.

1 Introduction

Ad-hoc wireless network is an ideal technology to establish an instant communication infrastructure for military applications in tactical environments. Many protocols have been proposed for efficient routing in multi-hop ad-hoc networks. Common ad-hoc routing pro-

ocols [31, 27, 20, 30] assume homogeneous networks where all nodes have the same transmission capabilities and use the same frequency and channel access scheme. These routing protocols do not scale well in terms of network size. For example, measurements of on-demand protocols [4] show that routing overhead grows as the traffic load increases. In the case of 100 nodes and 40 sources, the measurements show that on-demand routing protocols will generate much higher routing overhead than actual throughput capacity, and the maximum achievable throughput in the simulation scenarios is only 2-3% of total network capacity.

Recent studies [14, 15, 23] present the throughput bounds of homogeneous ad-hoc wireless networks. Under uniform traffic patterns, the available bandwidth to each networking node approaches zero as the network size increases. The fundamental reason is that each node has to share its bandwidth with neighboring nodes in broadcast wireless channel.

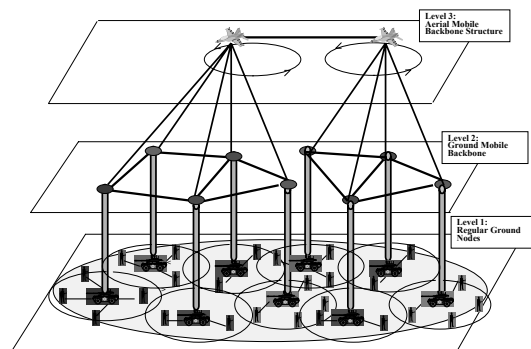


Figure 1. Hierarchical multi-layer ad-hoc wireless networks with Mobile Backbone (MBN) and Unmanned Aerial Vehicles(UAVs)

To overcome the above inherent limitations of homogeneous ad-hoc networks, heterogeneous multi-layer ad-hoc networks with UAVs, namely the UAV-MBN networks, have been recently proposed [13, 12, 11] to meet

the communication demands in future digital battlefields (see Figure 1 for an illustration).

1.1 UAV-MBN Networks

In a UAV-MBN network, there are three layers composed of three kinds of networking units with heterogeneous communication capability and computation power, the *regular ground mobile nodes*, the *ground mobile backbone (MBN) nodes*, and the *unmanned aerial vehicle (UAV) nodes*. Based on the availability of the UAV nodes, a UAV-MBN network may operate in two different communication modes: the *infrastructure mode* and the *infrastructureless mode*.

Regular ground nodes constitute the first layer. They are typically soldiers equipped with limited communication and computation devices. They communicate through bandwidth-constrained and range-limited broadcast wireless channel. The second layer consists of MBN nodes that are special ground fighting units such as trucks and tanks. They may carry a lot more facilities for stronger computation and communication power. With the beam-forming antennas, high-bandwidth point-to-point direct wireless links can be established between MBN nodes. These two ground layers form an ad-hoc wireless network with clustered hierarchy [24] where MBN nodes act as cluster heads. The network operates in the *infrastructureless mode* with these two ground layers when the third layer is absent.

The third layer is an aerial mobile backbone structure that consists of UAVs flying at an altitude of about 10 miles and in a circle with a diameter of around 10 miles. Each UAV leads a *single-area theater*. With the help of phased array antennas, it can provide the shared beam to its MBN nodes to maintain line-of-sight connectivity for one area of operations down below. All UAVs form the aerial mobile backbone that is employed to route inter-theater traffic. With UAVs, the network works in the *infrastructure mode* where intelligent and extremely efficient medium access [11] and routing [13, 12] are realized compared with homogeneous wireless ad-hoc networks.

1.2 Security of UAV-MBN Networks

Security support is a must for networks deployed in tactical environments. In general, five security aspects have been defined: message privacy, message integrity, non-repudiation, authentication, and security

service availability [42]. Cryptosystems and authentication protocols are employed in existing networks to address the five security concerns.

Both symmetric key cryptosystems and asymmetric key (aka. public key) cryptosystems have been successfully migrated from existing wired networks to wireless networks. For example, the Wireless Application Protocol (WAP) standard [46] is fully certification-based and instantiated on symmetric key and public key cryptosystems. Some recently made WAP-enabled cellular phones (e.g., Siemens S35i) have integrated RSA chips to communicate via the WAP protocol. As the cryptosystem implementations become less expensive and more mature on both hardware and software, communication devices in military battlefield are capable of operating in both symmetric key and public key cryptosystems.

For authentication services, current approaches assume centralized management by either key distribution centers (KDC) or certification authorities (CA). For UAV-MBN networks in digital battlefields, we may deploy centralized management in the third layer UAVs so that each UAV provides authentication services for its theater, and the aerial mobile backbone serves the entire system with inter-theater authentication. However, relying on the centralized resources suffers from single-point of service denial. When the UAVs are destroyed by missiles or hostile aircrafts, the system security breaks down if no backup scheme is implemented. A simple solution to this problem is to deploy redundant authentication servers in some ground units such as the second layer MBN nodes. However, this make-up suffers from single-point of compromise if any of these ground MBN nodes is broken in.

In this paper, we propose an adaptive security solution to address these issues, without sacrificing the efficiency, flexibility and strong security semantics of the centralized approaches. When the UAV is absent for any reason, the surviving ground units in the theater switch to the infrastructureless mode in terms of both communication and security. In the infrastructureless mode, the authentication services are distributed into each individual ground node's vicinity. Like its centralized counterpart, the distributed scheme effectively maintains authentication services in the theater until a new UAV is available and the theater switches back to the infrastructure mode. Transitions between these two different modes

are streamlined in a seamless fashion.

Our main contribution is to provide robust security services that adapt to dynamic infrastructure changes of the UAV-MBN network. We achieve seamless transitions between the two communication modes. A suit of algorithms and protocols are implemented to realize the design with practical intrusion detection mechanisms.

The rest of this paper is organized as follows. The assumptions are defined in § 2. Detailed design is presented in § 3. We evaluate implementation and simulation results in § 4. § 5 compares with related works and § 6 summarizes the paper.

2 Assumptions

As the communication infrastructure of ad-hoc networks is volatile and vulnerable to wide-range of attacks [51], it is inappropriate to push the complexity into the infrastructure. Thus by enforcing *end-to-end security* at the transport layer, we are able to provide solid and uniform security support to every node in the network despite security vulnerabilities in the lower layers. In our design, data privacy, data integrity, and data non-repudiation are realized by existing end-to-end security solutions as specified in SSL/TLS [26, 5] and its wireless extension WTLS [47]. Related cryptanalysis [45] has approved the overall design and also provided countermeasures to correct a number of minor flaws in the protocols.

In transport layer security, authentication is based on certification services as specified in public key infrastructure (PKI). We employ the *de facto* standard RSA [34] as the public key cryptosystem in our design. We assume RSA cryptographic primitives are secure, and brute-force break-ins of the RSA primitives are impractical. This can be realized by employing state-of-art countermeasures proposed by cryptanalysts [1] and using keys of enough length [22].

Nodes are assumed to be appropriately initialized before combat. During combat, any node, including the ground nodes and the UAVs, may be destroyed at any time. Besides, any ground nodes can be captured and compromised unpredictably. Once the incident happens to ground nodes, we assume all their security-related information is compromised and made available to the enemies. Nevertheless, given UAV's aerial positions and advanced tamper resistance technologies, we assume

they are not compromisable. For example, a UAV may implement a self-destruction mechanism when its altitude sensing and speed sensing units report misposition.

To ever make intrusion detection possible, we assume that the ground nodes can monitor and perceive local intrusions. Such local intrusion detection mechanisms do not require abrupt shifts from the methods currently used in tactical environments, where perception-based intrusion detection remains as the most effective and reliable means to authenticate intact units and isolate compromised units. In this paper we seek to provide robust end-to-end security support on top of localized intrusion detection and authentication schemes, such that (i) *A node can only be broken on its standing site. Any break-ins and compromises occurring en route do not compromise its data traffic, which is encrypted at transport layer before reaching the network;* and (ii) *Once a node is broken, effective and efficient mechanisms are employed to isolate it.*

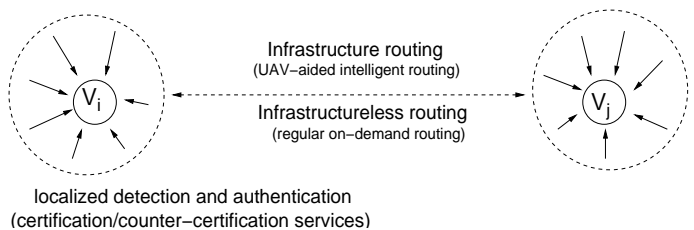


Figure 2. End-to-end Security with Localized Intrusion Detection and Security Services

3 Design

In this section, we present our detailed design that adapts to the changes of the network infrastructure. We describe the RSA-based authentication primitives in § 3.1. § 3.2 presents infrastructure mode and § 3.3 presents infrastructureless mode. We conclude in § 3.4 with discussions.

3.1 Primitives

Authentication via certificates In the theater α , each networking node v_i is associated with a personal RSA key pair $\{\overline{pk}_i, \overline{sk}_i\}$. \overline{pk}_i is v_i 's public key for encryption and verification. \overline{sk}_i is v_i 's private key for decryption and signing. For the purpose of authentication, v_i 's public key \overline{pk}_i has to be certified by the CA of its theater. Generally a certificate (denoted as $CERT_{\alpha,i}$) is

a statement (denoted as $cert_{\alpha,i}$) that is signed by theater α 's CA. The statement $cert_{\alpha,i} = \langle v_i, \overline{pk}_i, T_{sign}, T_{expire} \rangle$ may read: "It is certified that the personal public key of node v_i is \overline{pk}_i starting from the signing time T_{sign} until the expiration time T_{expire} ".

The CA of theater α holds an authoritative key pair $\{PK_\alpha, SK_\alpha\}$. In RSA, $PK_\alpha = \langle e_\alpha, n_\alpha \rangle$ and $SK_\alpha = \langle d_\alpha, n_\alpha \rangle$, with n_α as the modulo, e_α as the public exponent, and d_α as the secret exponent. A valid certificate is signed by SK_α

$$CERT_{\alpha,i} = (cert_{\alpha,i})_{SK_\alpha} = (cert_{\alpha,i})^{d_\alpha} \bmod n_\alpha.$$

The CA's public key PK_α is assumed to be well-known in the network. Other nodes verify the v_i 's certificate by applying PK_α to check if

$$cert_{\alpha,i} = (CERT_{\alpha,i})_{PK_\alpha} = (CERT_{\alpha,i})^{e_\alpha} \bmod n_\alpha.$$

Security services related to certification Certification services include certificate issuing, certificate renewal, certificate revocation, and storage/retrieval of certificates and certificate revocation list (CRL). A valid certificate has to pass two tests: (i) it is not expired, and (ii) it is not in the CRL.

We assume every node has obtained a valid certificate before it joins the UAV-MBN network. Valid certificates are used in WTLS [47] to enforce end-to-end transport layer security in wireless networks. In WTLS's class 3 authentication, both sender and receiver present and verify each other's certificates. A shared master secret is then established between them to derive cipher keys used in secure communication.

In ad-hoc networks, routing protocols are based on hop-by-hop packet forwarding. A node can be effectively isolated when all its neighboring nodes refuse to forward its packets. Thus by enforcing a data forwarding policy *for the authenticated nodes only*, nodes without valid certificates are isolated in the network.

3.2 Infrastructure Mode with UAV

With UAV's presence the theater α operates in the infrastructure mode. We propose an architecture of *centralized certification, centralized counter-certification and distributed local intrusion detection* for this mode.

The CA is implemented at the UAV to provide certification services for ground nodes in the theater (§ 3.2.1). Inter-theater authentication is achieved through the interactions among UAVs through the aerial mobile backbone (Figure 3). End-to-end secure communication is realized by transport layer security via WTLS (§ 3.2.3). Security states are maintained in the theater for transition to infrastructureless mode once the absence of its UAV is detected (§ 3.2.4).

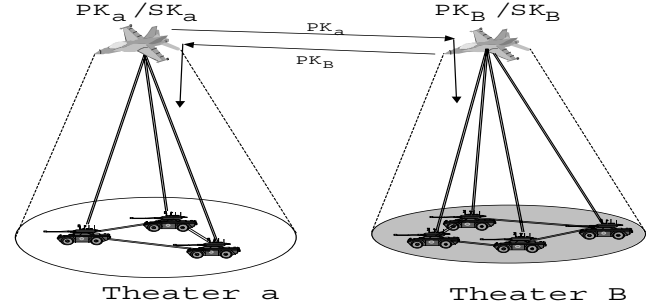


Figure 3. Security Configuration in UAV-MBN Network

3.2.1 Certification and Counter-certification

At the bootstrapping phase of the UAV-MBN network, every theater is equipped with a UAV and operates in infrastructure mode. The CA with key pair $\langle PK_\alpha, SK_\alpha \rangle$ is implemented at the UAV. Each CA's public key is well known in the network. Given N theaters in the network, our design requires each ground node store the corresponding N public keys. We discuss in § 3.4 on the storage issue for low-end ground nodes.

Certification is employed to authenticate intact nodes and isolate compromised nodes. The certificates held by the compromised nodes are revoked upon intrusion detections. We employ two complementary methods to achieve the goal.

1. *Implicit certificate revocation* by enforcing frequent certificate renewals in short periods.
2. *Explicit certificate revocation* by counter-certification.

In the case of implicit certificate revocation, a theater parameter T_{renew} is predefined in the theater to bound the valid time of all certificates. That is, $T_{expire} \leq (T_{sign} + T_{renew})$, a certificate holder must renew its certificate within T_{renew} . The appropriate value for T_{renew} depends on the UAV's computation power and the number of ground units in its theater.

In the case of explicit certificate revocation, compromised units are put into the theater CRL. On the Internet, normally a CRL is stored in a trusted centralized storage. If the CRL needs to be stored distributedly, an item in the CRL may be forged at each replication site. In our design we employ *counter-certificates* to solve this problem. Whenever a node v_x is considered to be defected, the CA signs a counter-certificate $\langle \perp v_x, T_{sign}^\perp \rangle_{SK}$ where \perp is a special tag for counter-certificates. By counter-certification nobody except the CA can generate an item in the CRL.

To ensure the access to the theater CRL, a CRL update (i.e., a new counter-certificate) is always flooded in the theater and each ground node maintains a local copy of the theater CRL. Even without reliable transmission mechanisms, the flooding can be implemented by one-hop wireless broadcast. Here we take advantage of the connectivity redundancy in a typical ad hoc network setup to ensure the reliability of the flooding.

CRL's storage requirements are optimized by the implicit revocation mechanism. Each node only needs to maintain a subset of counter-certificates within the past T_{renew} . That is, given a counter-certificate $\langle \perp v_x, T_{sign}^\perp \rangle_{SK_\alpha}$ and the current time NOW , a node must store the counter-certificate if $(T_{sign}^\perp + T_{renew} > NOW)$, or discard it otherwise.

3.2.2 Intrusion Detection

When a ground node v_x is compromised by enemy, each neighboring node v_i that perceives this incident sends an accusation to the theater CA. The accusation is signed with v_i 's private key sk_i as in " $\langle accusation, v_x \rangle_{sk_i}$ ". It is then delivered to the UAV together with v_i 's valid certificate. Once the UAV receives a certain number (K) of such accusations against v_x , it signs the counter-certificate toward v_x and broadcasts it in the theater.

The threshold K is a critical parameter of the theater. If somehow the enemy manages to capture and compromise K ground nodes before being detected by their neighbors, the enemy can generate false accusations from these K compromised nodes against intact nodes. The result is decided by a temporal competition between the intact community and the compromised but not-yet-revoked nodes. There is at least one advantage available to the intact community: the enemy will experience a non-trivial delay to compromise the captured

devices and then issue false accusations. Adding various tamper resistance mechanisms [3, 16] to wireless devices can further increase the delay, thus minimize the winning chance of the compromised nodes.

3.2.3 Intra-theater and Inter-theater Secure Communication

The first step toward secure communication is the authentication between two communicating ground nodes. In general, these two nodes need to verify each other's certificate using (1) the well-known theater public keys and (2) the *authentic up-to-date* theater CRLs (Figure 4). In this section we present our design for authentication between two nodes both from theaters operating in infrastructure mode. § 3.3.2 studies the scenarios where one or both nodes are from theaters operating in infrastructureless mode.

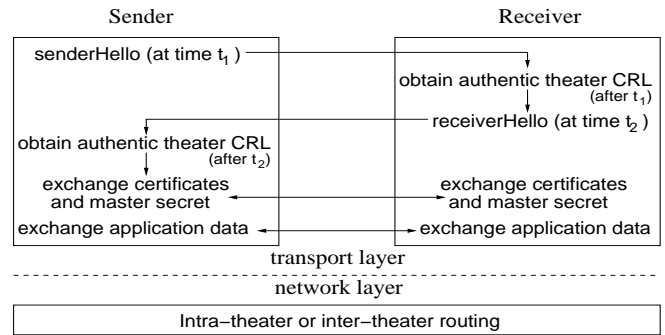


Figure 4. Enhanced WTLS Session Handshake

For intra-theater authentication, since the UAV always broadcasts the theater's up-to-date CRL, the step of exchanging authentic up-to-date CRL can be skipped since each node already has a local copy. Two ground nodes simply exchange their certificates to complete the authentication step.

When these two nodes are from different theaters, say node v_i from theater α and node v_j from theater β , each of them must provide the other node with the authentic and up-to-date CRL of its own theater. To get a up-to-date CRL of its theater α , node v_i has two options. It can either query its UAV so that the UAV combines all the counter-certificates and returns an SK -signed CRL with current timestamp to satisfy the timeliness requirement. Node v_i may also query its K neighboring ground nodes so that each of them returns a signed CRL with current timestamps. Both UAV-signed CRL and the K node-signed CRLs are considered to be authentic, where K

is set to be the same threshold in counter-certification. The second option can be applied when the UAV is under heavy load that results in large delay, or when the theater is in infrastructureless mode (§ 3.3.2). Node v_i then forwards the CRL(s) to node v_j . If K node-signed CRLs are received by v_j , v_j checks all of them to verify that v_i 's certificate is not revoked by any of these CRLs.

Ground nodes without valid certificates or having their certificates revoked are isolated. Their packets are dropped by other ground nodes or UAVs. On the contrary, two authenticated nodes can establish secure communication channels to ensure message privacy, integrity and non-repudiation. Depending on whether the two communicating nodes are in the same theater, intelligent intra-theater routing protocol [13] or multi-theater routing protocol [12] is employed with WTLS protocols to securely and efficiently exchange application data (Figure 4).

3.2.4 Transition to Infrastructureless Mode

Although both communication and authentication in infrastructure mode feature efficiency with low overhead and flexibility as in a centralized system, the infrastructure is vulnerable to attacks. Deploying UAV-MBN networks in hostile environments has to handle the situation when the UAV becomes unavailable for any reason. A naive make-up is to replicate the theater CA to some ground nodes. However, as each replicated CA is exposed to unpredictable compromises on the ground, this scheme sacrifices the overall security level due to single-point of compromise.

Based on Shamir's secret sharing [38], our solution is to distribute the certification services into each ground node when the theater is operating in infrastructureless mode without UAV. As the result, a localized coalition with a threshold number (K) of members collaboratively provides authentication services to its locality, while the system tolerates up to $K - 1$ break-ins. Due to the inherent local connectivity redundancy of ad-hoc networks, each ground node can receive highly available authentication services from its vicinity. The threshold parameter K is set to the same number in counter-certification in order to maintain a comparable security level as in the infrastructure mode. We present the service instantiation for infrastructureless mode in § 3.3.1.

Smooth transition to infrastructureless mode is ac-

complished by a backup scheme. Occasionally, theater α 's UAV generates a *backup authoritative key pair* $\langle PK'_\alpha, SK'_\alpha \rangle$. We name $\langle PK_\alpha, SK_\alpha \rangle$ as the UAV's *primary authoritative key pair* to differentiate with its backup key pair.

- As what has been done to the primary verification key PK_α , the backup verification key PK'_α is advertised and well known in the network.
- The backup signing key SK'_α is shared among the ground nodes in the theater. By end-to-end secure channels, each authenticated node v_i obtains a secret share $SK'_{(\alpha,i)}$ from the UAV. Since unauthenticated nodes cannot establish end-to-end secure channels without valid certificates, they are disqualified being secret share holders.

This process creates a backup *distributed certification authority (DCA)* in theater α that will be functional in the infrastructureless mode. Each ground node will have to maintain the primary and the backup public keys for every theater, resulting in $2 \cdot N$ public-key storage requirement given N theaters in the network (§ 3.4).

In Shamir's scheme, compromises of K secret shares will expose the backup signing key, thus the UAV must update the theater's backup key pair for every K detected compromises. Switching to infrastructureless mode is triggered by the absence of the UAV, which may be detected by a timeout-based UAV beaconing or line-of-sight perception. At the absence of UAV, the theater switches to infrastructureless mode and the backup SK'_α starts to function as the official signing key.

3.3 Infrastructureless Mode without UAV

We propose an architecture of *distributed certification*, *distributed counter-certification* and *distributed local intrusion detection* when the theater is operating in infrastructureless mode. The functionality of certification authority is distributed among each surviving ground node. Local coalition of K ground nodes collaboratively provides services to a certification request (§ 3.3.1). Intra-theater and inter-theater authentication are presented in (§ 3.3.2). The transition to infrastructure mode is studied in (§ 3.3.3).

3.3.1 Distributed Certification Services

Given the size of network N , a system parameter K ($0 < K \leq N$), and a centralized CA with RSA key pair $\{SK'_\alpha, PK'_\alpha\}$, cryptographic algorithms [8, 36, 33, 39, 21] and systems [49, 52, 53] allow the functionality of the CA to be distributed into the network where each node becomes a partial CA. Each partial CA holds a secret share $SK'_{\alpha,i}$ ($1 \leq i \leq N$), and a coalition of any K -out-of- N partial CAs can function as the centralized CA. During the certification process each partial CA in the coalition signs a partial certificate with its secret share, the complete certificate can be obtained by combining the K partial certificates.

Such a de-centralized scheme is able to find a balance point between service availability and intrusion tolerance. The adversaries must turn off $(N - K + 1)$ partial CAs to turn off certification services, while they must break in K partial CAs to steal the signing key SK'_α .

Further contributions on proactive secret share updates [17, 10, 9, 33], verifiable secret sharing [6, 41, 37], and fully-distributed DCA [21] offer more security warranties in applying the de-centralized scheme in the context of scalable networks with long-term adversaries and untruthful coalition members. In a scalable network with large number of secret share holders, not only the secret shares $\{SK'_{\alpha,i} | 1 \leq i \leq N\}$ can be proactively refreshed to resist break-ins, but also signing a message with a fake secret share can be detected publicly or by the service requester.

Compared to the above scheme, a naive CA-replicating scheme would reveal SK'_α once a single site is compromised. A KDC-based authentication scheme [7, 43] lacks background and experience to distribute system secrets to multiple nodes, while both service availability and intrusion tolerance must be guaranteed.

We employ the distributed CA in the infrastructureless mode. The cryptographic details are presented in the Appendix. In a theater operating in the infrastructureless mode, node v_i 's certification request is served by a local coalition of K secret share holders. After each coalition member signs and returns a partial certificate, v_i is able to obtain an SK'_α -signed certificate as if the centralized CA presents in its locality.

Counter-certification is similar to the certification process. Once a compromised ground node v_x is detected by its neighbors, each of them signs a partial

counter-certificate against v_x . A full counter-certificate is generated by combining K such partial counter-certificates. Then it is flooded in the theater so that other nodes in the theater can update their CRL caches.

3.3.2 Intra-theater and Inter-theater Secure Communication

As in the infrastructure mode, end-to-end secure channels can be established if both ends hold valid certificates. For intra-theater communications, the step of exchanging CRLs can be skipped because the theater CRL is already locally cached.

For inter-theater communications, two scenarios are possible. In the first scenario one node is from a theater operating in infrastructure mode and the other from a theater operating in infrastructureless mode. In the second scenario both parties are from theaters operating in infrastructureless mode. In either scenarios,

- If a node is from a theater operating in the infrastructure mode, it may choose either of the two alternatives described in § 3.2.3 to acquire authentic and up-to-date theater CRL.
- If a node is from a theater operating in the infrastructureless mode, it has to query K other nodes in the same theater in the absence of UAV, typically among its neighbors. Each of these K nodes returns a signed CRL with current timestamp to satisfy the timeliness requirement. The communication peer verifies that the node's certificate is not revoked by any of these K CRLs.

3.3.3 Transition to Infrastructure Mode

Ground nodes that belong to a theater in infrastructureless mode may join other theaters with UAVs for more efficient communication. Besides, a new UAV with original SK_α may be available so that the theater can switch back to infrastructure mode. The new UAV firstly broadcasts an SK_α -signed hello message in the theater to claim authority, then it has to obtain the authentic and up-to-date CRL.

- The new UAV can obtain signed-CRLs from exactly K surviving ground nodes with appropriate certificates. If the certificate of *any* of these K nodes is revoked by the result CRL, the procedure has to restart again.

- Or the new UAV can obtain signed-CRLs from more than K surviving ground nodes, then picks out a set of K nodes such that none of their certificates is revoked by the K CRLs they signed.

After the new UAV claims authority and obtains authentic up-to-date CRL of the theater, it can provide efficient security services to all surviving ground units.

3.4 Discussions

In this section, we comments on several issues.

3.4.1 Protecting backup certificate signing key SK'_α

In the infrastructure mode, UAV maintains the backup DCA by distributing the backup certificate signing key SK'_α in the theater. The backup DCA key pair is occasionally updated for every K compromised ground nodes. In the infrastructureless mode, it is ineffective to generate and renew the backup DCA key pair due to lack of central management¹. Fortunately, proactive secret share update [17, 10, 9, 33] and self-initialization [21] allow the network to periodically update all the secret shares without compromising the shared secret. As long as there are less than K ground nodes broken between two consecutive secret share updates, the backup signing key SK'_α is protected against break-ins and can remain unchanged throughout.

3.4.2 Threshold K

The threshold K affects our system in the following aspects:

- *Intrusion tolerance:* In the infrastructureless mode, if the enemy is able to break K nodes between two consecutive share updates, the backup DCA signing key SK'_α is compromised. Various tamper resistance mechanisms [3, 16] can be further applied to increase the level of intrusion tolerance.
- *Certification service availability:* In the infrastructureless mode, the communication overhead is minimal when a ground node has at least K one-hop

partial CAs. Otherwise, any of the partial CA can serve as a proxy and use its own trust to bring in more partial CAs, though the communication overhead is increased in this scenario.

- *False accusations:* As described before, K should be appropriately chosen so that the intact community outperforms the not-yet-revoked defected nodes. Obviously K must be greater than the expected number of nodes involved in a captivity. Battlefield statistics are helpful in finding an appropriate value, and adding tamper resistant mechanism to mobile devices helps to decrease the value.
- *Counter-certification overhead:* In either mode, K valid accusations or K partial counter-certificates are needed to revoke a certificate. The overhead of counter-certification increases as a larger K is adopted.

In military environments, the privilege for every node is inherently hierarchical and heterogeneous. For example, a lieutenant usually hold more confidential information than a private. This implies that an asymmetric function sharing model is more reasonable. In UAV-MBN networks, the MBN nodes could hold more shares of the backup DCA than common soldiers. If an MBN node holds $k - 1$ shares, it only needs another regular ground mobile node to function as the backup DCA. However, breaking the MBN nodes also results in more damage on security services.

3.4.3 Less than K neighbors

So far we assume that the requesting entity has at least K one-hop neighbors. In the simulation described in § 4.2, every requesting entity broadcasts the requests for a limited number of times (e.g., 2-3) over a time window to “accumulate” enough number of neighbors, even if at any time constant it does not have K neighboring nodes. In this scenario the node mobility actually helps providing certification services. Besides, in tactical mobile networks group mobility [18, 29, 28] is considered a valid mobility model where a group of network entities randomly roam together within certain distance. Appropriate group sizes can be chosen according to the threshold K .

Initial certification of a new node and re-certification of a node with less than K neighbors can also be built

¹Though shared key-generation schemes are available in literatures [2, 25], the result key pair is revealed to the key-generation requester. Besides, it is an open question who has the authority to annul current signing key.

on top of the perception-based intrusion detection, as we assumed in Section 2. As long as *a node has already been identified* as being “good”, its neighbors, even if they are more than one-hop away, can participate and issue a valid new certificate to it. In the scenarios where a compromised node has less than K uncompromised neighbors, no counter-certificate can be signed against it. However, its current certificate will expire in less than T_{renew} time, and it cannot obtain a new valid certificate after that.

3.4.4 Storage Requirements

The theater CRL, the primary public keys, and the backup public keys of all theaters are required to be locally stored at each node. From our empirical experience, the size of a public key or a counter-certificate is normally in the range of 128 to 256 bytes (as for RSA signing key length 1024 to 2048 bit). Given the typical size of a theater $0 < N < 1000$ and the probability of compromise $0 \leq P \leq 1$, the storage required for system CRL and public keys is acceptable for most low-end devices ($\sim 200k$ bytes). Besides, the implicit revocation mechanism helps to reduce the storage requirement significantly (§ 3.2.1).

The storage requirement can be further optimized with standard features available in WTLS [47], where a URL-based access method has been invented to relieve low-end devices from storing information locally. In particular, low-end devices can put information on trusted nodes with enough storage, then use short URLs to refer to the resources. In our system where WTLS is implemented, a low-end node manages to store information locally, otherwise it has to depend on storage resources on other local nodes. This can be realized on the cluster-head MBN nodes, or even the UAV. The compromises of MBN nodes or the failure of UAV may hurt the availability of these public informations, but not the overall system security level since no secret information is exposed. The affected nodes can obtain the public informations from its neighborhood at real time, as described in § 3.3.2.

4 Evaluation of Implementation and Simulation

We have implemented our design on both UNIX platforms and a popular network simulator *GloMoSim* [44].

Table 1. Testbed configuration

Host	CPU	O.S.	SPECint1995
H1	microSPARCII 85M	Solaris2.7	1.3
H2	PentiumII 300M	RedHat 6.2	12
H3	PentiumIII 500M	RedHat 6.2	21
H4	PentiumIII 850M	RedHat 6.2	39

In this section we will first evaluate computation overheads of our cryptographic implementations on heterogeneous UNIX platforms, then evaluate network communication overheads and the impact of mobility by our UAV-MBN implementation in GloMoSim simulator.

4.1 Computational Measurements and Evaluation

We have realized the standard transport layer security protocol WTLS [47] and the fully-distributed backup DCA in our implementation. We use SPECint [40] metrics to differentiate computation power on heterogeneous platforms. The testbed we employed is shown in Table 1, where $H_{i, 2 \leq i \leq 4}$ represents heterogeneous computation power from various mobile laptops, and H_1 's computation power is less than popular portable computing devices such as iPaq².

Table 2. Measurements of Computation Delay in RSA cryptosystem

key length (bit)	PK -verification (10^{-3} second)				SK -signing (second)			
	H1	H2	H3	H4	H1	H2	H3	H4
768	4	2	1	1	0.640	0.031	0.017	0.010
1024	4	2	1	1	1.295	0.066	0.039	0.019
1280	4	2	1	1	2.461	0.121	0.067	0.037
1536	4	3	1	1	3.854	0.172	0.109	0.059

We use RSA cryptographic primitives to realize the public key cryptosystem in our design. The result shown in Table 2 illustrates the performance of RSA cryptosystem are not prohibitively expensive even for the low-end device. Thus leveraging PKI-based approaches into wireless ad-hoc networks is an acceptable solution.

Table 3 and 4 illustrate the computation overhead of our distributed certification services under typical cryptographic and network settings. In Table 3, various values for the length of signing key SK'_α are selected, while

²Though there is no official SPECint result measured for iPaq's StrongARM CPUs, results obtained from industry (e.g., <http://n0cgi.distributed.net/statistics/stats.html>) show that SPECint95 value for StrongARM/206M CPU falls in the range between 3 and 6.

Table 3. Measurements of Computation Delay in backup DCA (Varying CA's signing key length, $K = 5$, result unit: second)

CA's key (bit)	Sign a Partial Certificate (as a coalition member)				Combine Partial Certificates (as a service requester)			
	H1	H2	H3	H4	H1	H2	H3	H4
768	1.48	0.08	0.04	0.02	1.65	0.09	0.04	0.02
1024	3.17	0.17	0.08	0.05	3.33	0.19	0.09	0.06
1280	5.55	0.30	0.15	0.09	5.90	0.33	0.17	0.09
1536	10.13	0.79	0.25	0.15	10.43	0.53	0.27	0.16

Table 4. Measurements of Computation Delay in backup DCA (Varying system parameter K , CA's signing key length=1024bit, result unit: second)

K	H1		H3	
	SPC	Combine	SPC	Combine
2	2.991	3.304	0.079	0.094
3	2.998	3.293	0.080	0.096
5	3.174	3.328	0.080	0.096
7	3.163	3.530	0.082	0.099
10	3.099	3.394	0.081	0.098
20	3.078	3.458	0.080	0.100
30	3.082	3.410	0.080	0.098

K is kept as a constant in typical network scenarios. Our measurements show that computation power is a critical factor that affects the efficiency of our design, although for typical scenarios the performance is acceptable (assuming nowadays typical RSA key length 1024 and 1280).

A major computation overhead owes to exponentiation on large numbers. We observe that the standard RSA SK -signing is almost 2.5 times faster than signing a partial certificate or combining K partial certificates. This is due to a major optimization technique employed in PKCS#1 standard [35] when every secret parameter in RSA signing key is known (i.e., d, p, q as for $SK = \langle d, n \rangle$ and the RSA modulo $n = p \cdot q$). The Chinese remainder theorem allows the RSA algorithm to decrease the exponentiation on the large private exponent d to smaller exponents with values less than $p - 1$ and $q - 1$, thus significantly decrease the computation overhead. When p and q are not available, such optimization technique cannot be used.

In Table 4, various values for K are selected, while CA's signing key length is kept as a typical value. The measurements show that the variation of K has small impact on the computation delay for certification services, since the K partial certificates are signed in parallel by the coalition members.

Table 5 shows the computation overhead in establishing an end-to-end secure channel between arbitrary two

Table 5. Measurements of Computation Delay for Authentication and Cipher Key Exchange in WTLS Session Handshake (result unit: second)

my key length (bit)	Client Side (WTLS class 3)				Server Side (WTLS class 2 & 3)			
	H1	H2	H3	H4	H1	H2	H3	H4
768	0.51	0.03	0.02	0.01	0.64	0.04	0.02	0.02
1024	1.01	0.06	0.03	0.02	1.29	0.07	0.03	0.02
1280	1.80	0.11	0.05	0.03	2.46	0.14	0.06	0.03
1536	2.84	0.16	0.08	0.05	3.85	0.22	0.11	0.06

nodes. By enforcing WTLS authentication class 3 in the UAV-MBN network, both sides must do authentication by presenting valid certificates. The authentication delay incurred is only a one-time cost for each session. The measurements show that the one-time cost is acceptable since the users need not tolerate more than 10 seconds session startup delay. After then a secure channel is established between the two ends. Cryptanalysis [45] has shown that the SSL/TLS/WTLS protocol is robust against attacks.

4.2 Communicational Measurements and Evaluation

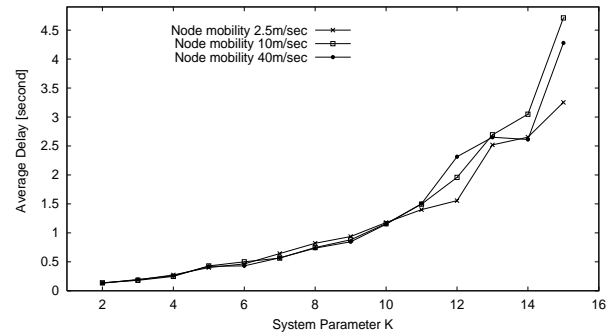


Figure 5. Average Certification Delay

Our simulation environment for UAV-MBN network is GloMoSim and hierarchical landmark [50]. We model a single theater in infrastructureless mode with 1000 ground nodes placed randomly within a 3200m×3200m area. Among them 100 are MBN nodes with point-to-point direct wireless link of 800m transmission range. Others are regular nodes with broadcasting wireless link of 175m range.

Performance is measured for certification service over the entire backbone where each node periodically issues a certification service request. In particular, whenever a request is issued, the next request is scheduled to be

issued at the middle point between the current clock time and the certificate expiration time. Therefore, (i) if this request fails, then the subsequent tries of the same request are repeated more frequently as the clock approaches the expiration time; or (ii) if this request succeeds, then the first renewal request is scheduled at the middle point of the new certificate's valid time.

The assumed backup signing key length is 1024 bit and the assumed computation power corresponds to $SPECint95 = 20.5$. Each request is served within one-hop neighborhood only as no routing scheme is employed. The first set of experiments in Figure 5 shows the average delay of the certification services. With various K values at typical roaming speeds (2.5m/sec, 10m/sec, 40m/sec), the average service delay for a certification request increases as the value K grows. This is because extra efforts are demanded to collect more partial certificates. When K is greater than a critical value (14 in the scenario), it is prohibitively difficult to find enough neighbors, thus the system performance degrades.

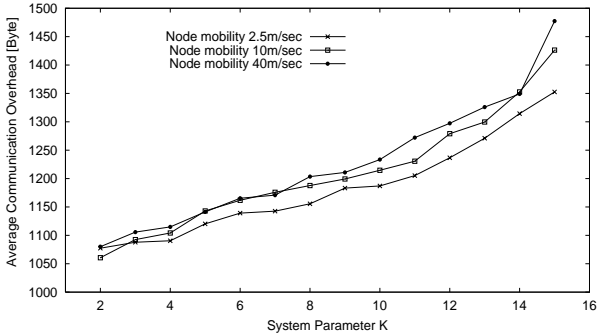


Figure 6. Average Certification Overhead

In Figure 6, we study the impact of certification service on the bandwidth of this UAV-MBN network. With various K values under typical roaming speeds, the results show that the overall certification overhead of all nodes increases linearly as K increases, since more partial certificates need to be collected, and the number of partial certificates increases linearly as analyzed in § 3.4.2.

After a K -coalition is formed, communication among them may fail due to the reasons like node mobility and wireless channel errors. In Figure 7, we study the success ratio of certification requests as a function of value K . The result shows that 100 percent ratio is achieved for reasonable K values. Once K grows over a crit-

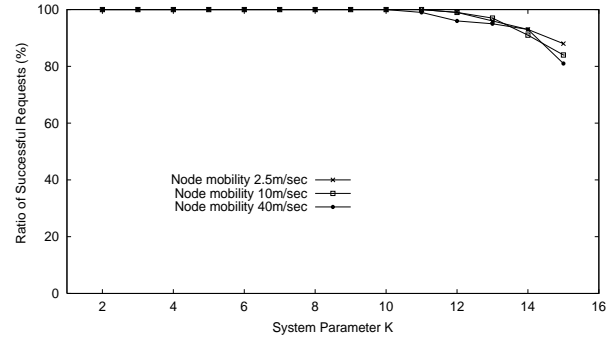


Figure 7. Certification Request Success Ratio

ical value (11 in the scenario), more certification requests will fail as it is more difficult to maintain the K -coalitions.

The simulation confirms that the one-hop certification design is insensitive to varying mobility in UAV-MBN networks with reasonable configuration, thus is ready to realize end-to-end communication security for the roaming entities in battlefields.

5 Related Works

Some popular network security services are provided by Kerberos [43], PGP [32] and X.509 Directory Authentication Service [19]. In these proposals, services are typically achieved via a centralized CA. Challenges from service availability, node mobility, and network scalability are not fully responded. For example, Charon [7] is an implementation of authentication services based on Kerberos. It addresses the device heterogeneity in wireless networks by deploying an infrastructure with base stations and placing the complexity into the infrastructure. Though mobile clients, especially those running low-end devices, can spend less computation power in authentication services, the authentication server end still suffers the single point of compromise and single point of failure/DoS attack.

Threshold-based secret sharing [38, 17, 36] and proactive secret share updates [17, 10, 9] have been very active topics in cryptography research. However, most of these proposals target a system that has a few secret share holders with reliable and rich connections. Hence, the proposed solutions are more suitable to wireless networks with base station-like infrastructure [52, 53]. Though they solve the problem of single point of failure and compromise, the other important issues, such as node mobility, wireless channel errors over multi-

hop path, and scalability, are not addressed, as admitted in [3]. For wireless ad-hoc networks operating in hostile environments, the security schemes cannot adapt to the destruction of the infrastructure. Besides, as connections are assumed to be reliable, they do not make explicit efforts to minimize communication overhead. In contrast, our adaptive solution works under very weak network assumptions.

6 Future work & Conclusions

In this paper, we propose a security framework for UAV-MBN networks in hostile environments such as battlefields. Our design adapts to the dynamical infrastructure changes of the network, depending on the availability of UAVs. Centralized design is employed with UAVs to achieve efficiency and flexibility when a theater is operating in infrastructure mode. In the scenarios where the UAV is destroyed by enemies, the system switches to infrastructureless mode where distributed security function sharing is applied to maintain comparable certification services and intrusion detection. As a potential part of the UCLA ONR MinuteMan project, we are improving our prototype design and exploring the possibility to integrate our security design with practical routing and other networking solution used in battlefields.

References

- [1] D. Boneh. Twenty Years of Attacks on the RSA Cryptosystem. *Notices of the American Mathematical Society*, 46(2):203–213, 1999.
- [2] D. Boneh and M. K. Franklin. Efficient Generation of Shared RSA Keys. In *CRYPTO*, pages 425–439, 1997.
- [3] R. Canetti, S. Halevi, and A. Herzberg. Maintaining Authenticated Communication in the Presence of Break-Ins. *Journal of Cryptology*, 13(1):61–105, 2000.
- [4] S. R. Das, C. E. Perkins, and E. E. Royer. Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks. In *INFOCOM*, pages 3–12, 2000.
- [5] T. Dierks and C. Allen. The TLS Protocol, version 1.0. <http://www.ietf.org/rfc/rfc2246.txt>, 1999.
- [6] P. Feldman. A Practical Scheme for Non-interactive Verifiable Secret Sharing. In *FOCS*, pages 427–437, 1987.
- [7] A. Fox and S. D. Gribble. Security on the Move: Indirect Authentication using Kerberos. In *MOBICOM*, pages 155–164, 1996.
- [8] Y. Frankel and Y. G. Desmedt. Parallel Reliable Threshold Multi-signature. Technical Report TR-92-04-02, Dept. of EECS, University of Wisconsin-Milwaukee, 1992.
- [9] Y. Frankel, P. Gemmell, P. MacKenzie, and M. Yung. Optimal Resilience Proactive Public-Key Cryptosystems. In *FOCS*, pages 384–393, 1997.
- [10] Y. Frankel, P. Gemmell, P. MacKenzie, and M. Yung. Proactive RSA. In *CRYPTO*, pages 440–454, 1997.
- [11] D. L. Gu, H. Ly, X. Hong, M. Gerla, G. Pei, and Y. Lee. C-ICAMA, A Centralized Intelligent Channel Assigned Multiple Access for Multi-layer Ad-hoc Wireless Networks with UAVs. In *IEEE WCNC*, pages 879–884, 2000.
- [12] D. L. Gu, G. Pei, H. Ly, M. Gerla, and X. Hong. Hierarchical Routing for Multi-layer Ad-hoc Wireless Networks with UAVs. In *IEEE MILCOM*, 2000.
- [13] D. L. Gu, G. Pei, H. Ly, M. Gerla, B. Zhang, and X. Hong. UAV-aided Intelligent Routing for Ad-hoc Wireless Network in Single-area Theater. In *IEEE WCNC*, pages 1220–1225, 2000.
- [14] P. Gupta and P. R. Kumar. The Capacity of Wireless Networks. *IEEE Transactions on Information Theory*, IT-46(2):388–404, 2000.
- [15] P. Gupta and P. R. Kumar. Internets in the Sky: The Capacity of Three Dimensional Wireless Networks. *Communications in Information and Systems*, 1(1):39–49, 2001.
- [16] J. Hastad, J. Jonsson, A. Juels, and M. Yung. Funkspiel Schemes: an Alternative to Conventional Tamper Resistance. In *ACM CCS*, 2000.
- [17] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive Secret Sharing or: How to Cope with Perpetual Leakage. extended abstract, IBM T.J. Watson Research Center, November 1995.
- [18] X. Hong, M. Gerla, G. Pei, and C.-C. Chiang. A Group Mobility Model for Ad Hoc Wireless Networks. In *ACM/IEEE MSWiM*, pages 53–60, 1999.
- [19] International Telecommunication Union. Recommendation X.509(11/93) The Directory: Authentication Framework.
- [20] D. B. Johnson and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In Imielinski and Korth, editors, *Mobile Computing*, volume 353. Kluwer Academic Publishers, 1996.
- [21] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang. Providing Robust and Ubiquitous Security Support for Wireless Mobile Networks. In *ICNP*, pages 251–260, 2001.
- [22] A. K. Lenstra and E. R. Verheul. Selecting Cryptographic Key Sizes. *Public Key Cryptography*, pages 446–465, 2000.
- [23] J. Li, C. Blake, D. D. Couto, H. I. Lee, and R. Morris. Capacity of Ad Hoc Wireless Networks. In *MOBICOM*, 2001.

- [24] C. R. Lin and M. Gerla. Adaptive Clustering for Mobile Wireless Networks. *IEEE Journal of Selected Areas on Communications*, 15(7):1265–1275, 1997.
- [25] M. Malkin, T. Wu, and D. Boneh. Experimenting with Shared Generation of RSA keys. In *Internet Society's Symposium on Network and Distributed System Security (SNDSS)*, pages 43–56, 1999.
- [26] Netscape Communications Corporation. SSL 3.0 Specification.
- [27] V. D. Park and M. S. Corson. Temporally-Ordered Routing Algorithm (TORA) version 1: Functional Specification, 1998.
- [28] G. Pei, M. Gerla, X. Hong, and C.-C. Chiang. A Wireless Hierarchical Routing Protocol with Group Mobility. In *IEEE WCNC*, 1999.
- [29] G. Pei, X. Hong, and M. Gerla. LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility. In *IEEE/ACM MobiHOC*, 2000.
- [30] C. E. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In *SIGCOMM*, pages 234–244, 1994.
- [31] C. E. Perkins and E. M. Royer. Ad-hoc On Demand Distance Vector (AODV) Routing, 1998.
- [32] PGPi Project. <http://www.pgp.org/>.
- [33] T. Rabin. A Simplified Approach to Threshold and Proactive RSA. In *CRYPTO*, pages 89–104, 1998.
- [34] R. L. Rivest, A. Shamir, and L. M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *CACM*, 21(2):120–126, 1978.
- [35] RSA Security Inc. PKCS #1 - RSA Cryptography Standard. <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/>.
- [36] A. D. Santis, Y. Desmedt, Y. Frankel, and M. Yung. How to Share a Function Securely (Extended Summary). In *STOC*, pages 522–533, 1994.
- [37] B. Schoenmakers. A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting. In *CRYPTO*, pages 148–164, 1999.
- [38] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.
- [39] V. Shoup. Practical Threshold Signatures. In *EUROCRYPT*, pages 207–220, 2000.
- [40] Standard Performance Evaluation Corporation. <http://www.specbench.org>.
- [41] M. Stadler. Publicly Verifiable Secret Sharing. In *EUROCRYPT*, pages 190–199, 1996.
- [42] W. Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice-Hall, 2nd edition, 1999.
- [43] G. Steiner, B. C. Neuman, and J. I. Schiller. Kerberos: An Authentication Service for Open Network Systems. In *USENIX Winter*, pages 191–202, January 1988.
- [44] UCLA Parallel Computing Laboratory and Wireless Adaptive Mobility Laboratory. GloMoSim: A Scalable Simulation Environment for Wireless and Wired Network Systems. <http://pcl.cs.ucla.edu/projects/gloimosim/>.
- [45] D. Wagner and B. Schneier. Analysis of the SSL 3.0 protocol (revised version). In *2nd USENIX Workshop on Electronic Commerce*, 1996.
- [46] WAP Forum. Wireless Application Protocol. <http://www.wapforum.org/>.
- [47] WAP Forum. Wireless Transport Layer Security Specification. <http://www1.wapforum.org/tech/documents/WAP-261-WTLS-20010406-a.pdf>.
- [48] M. J. Wiener. Performance Comparison of Public-Key Cryptosystems. *RSA CryptoBytes*, 4(1):1–5, 1998.
- [49] T. Wu, M. Malkin, and D. Boneh. Building Intrusion Tolerant Applications. In *Eighth USENIX Security Symposium (Security '99)*, pages 79–91, 1999.
- [50] K. Xu, X. Hong, H. Ly, M. Gerla, and D. L. Gu. Landmark Routing In Large Wireless Battlefield Networks Using UAVs. In *IEEE MILCOM*, 2001.
- [51] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In *MOBICOM*, 2000.
- [52] L. Zhou and Z. J. Haas. Securing Ad Hoc Networks. *IEEE Networks*, 13(6):24–30, 1999.
- [53] L. Zhou, F. B. Schneider, and R. van Renesse. COCA: A Secure Distributed On-line Certification Authority. Technical Report 2000-1828, Computer Science Department, Cornell University, 2000.

A Polynomial sharing of SK'_α

We adopt the polynomial secret sharing to share SK'_α among the theater α . Let n be the RSA modulo of theater α 's backup certification key pair $\{PK'_\alpha = \langle e, n \rangle, SK'_\alpha = \langle d, n \rangle\}$. In our algorithm, ground node v_i 's polynomial share P_{v_i} and its additive share SK_{v_i} in term of a specific coalition, are defined over the ring Z_n , instead of $Z_{\phi(n)}$ or $Z_{\lambda(n)}$ as the previous works [8, 36, 33, 39] did. In the infrastructure mode (§ 3.2.4), the UAV chooses a random polynomial $f(x) = d + f_1x + \dots + f_{K-1}x^{K-1}$ where $f(0) = d$ and $\{f_1, \dots, f_{K-1}\}$ are uniformly distributed random numbers over a finite field. The UAV then private sends each ground node with its ID $v_i \neq 0$ a polynomial share $P_{v_i} = (f(v_i) \bmod n)$. By this means we eliminate the insecurity of releasing $\phi(n)$ or $\lambda(n)$. Moreover, with the K -bounded coalition offsetting that is presented below, we make the conversion from polynomial shares to additive shares scalable to the overall theater size. Only the IDs and shares of the participating K nodes are involved.

B Localized Multi-signature

Ground node v_i firstly chooses a coalition of K nodes from its neighborhood. Without loss of generality, let the coalition be $\mathcal{B} = \{v_1, v_2, \dots, v_K\}$. Note that node v_i itself can also be in the coalition if it is a secret share holder, hence needs only $K - 1$ neighboring share holders. v_i broadcasts the request, together with the IDs of these K nodes. Once a node $v_j \in \mathcal{B}$ receives the request and decides to serve the request, it firstly translates its secret share P_{v_j} into its Lagranged secret share SK'_{α, v_j} :

$$SK'_{\alpha, v_j} = (P_{v_j} l_{v_j}(0) \pmod n),$$

where the Lagrange coefficient l_{v_j} in the coalition is defined as $l_{v_j}(x) = \frac{(x-v_1)\dots(x-v_{j-1})(x-v_{j+1})\dots(x-v_K)}{(v_j-v_1)\dots(v_j-v_{j-1})(v_j-v_{j+1})\dots(v_j-v_K)}$.

Lagrange interpolation ensures that

$$d = \left(\sum_{j=1}^K SK'_{v_j} \pmod n \right). \quad (1)$$

For arbitrary number/message M , the following formula holds in arithmetic:

$$M^{SK'_{v_1}} \cdot M^{SK'_{v_2}} \dots M^{SK'_{v_K}} = M^{SK'_{v_1} + SK'_{v_2} + \dots + SK'_{v_K}}.$$

We would be able to obtain M^d from the product $\prod M^{SK'_{v_j}}$.

C K -bounded coalition offsetting

In the Equation 1, the sum of Lagrange interpolation $(\sum_{j=1}^K SK'_{v_j} \pmod n) = t \cdot n + d$ for certain t . However, there is no mathematical identity ensures that the result of the multiplicative multi-signature equals the SK'_{α} -signed message:

$$M^{t \cdot n + d} \equiv M^{t \cdot n} \cdot M^d \not\equiv 1 \cdot M^d \equiv M^d \pmod n.$$

Fortunately, each $SK'_{v_j} = (P_{v_j} \cdot l_{v_j}(0) \pmod n)$ is a value between 0 and $n - 1$ due to modular arithmetic. Thus t satisfies the inequation $0 \leq t \leq K$. After Algorithm 1 we are able to recover M^d by the help from the original message M and the system public key $PK = \langle e, n \rangle$.

In an ad-hoc network K is a small number corresponding to number of nodes in a neighborhood. Thus the loop in Algorithm 1 ends within reasonable rounds. Also it is well-known that PK -verification in RSA is

Algorithm 1 K -bounded Coalition Offsetting

Require: $Y \equiv M^{\sum_{i=1}^K (P_{v_i} \cdot l_{v_i}(0) \pmod n)} \equiv M^{t \cdot n + d} \pmod n$
is the product of all partial certificates.

```

1:  $Z := M^{-n} \pmod n$ 
2:  $j := 0$ 
3: while  $j \leq K$  do
4:   if  $(M \equiv Y^e \pmod n)$  then
5:     Success, break the loop
6:   end if
7:    $Y := Y \cdot Z \pmod n$ 
8:    $j := j + 1$ 
9: end while

```

Ensure: $Y \equiv M^d \pmod n$

an inexpensive operation [48]. The complexity of K -bounded coalition offsetting is the sum of $O(1)$ exponentiation, $O(k)$ modular multiplications, and $O(k)$ RSA PK -verifications.