International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-4)

Research Article | **April 2014**

Key Management Scheme in Mobile Ad Hoc Networks

Abu Taha Zamani[1], Syed Zubair[2]
[1]*Research Scholar, Techno Global University, Shillong, Meghalaya, India*
[2]*Assistant Professor, Department of Information Technology, Nawab Shah Alam Khan College of Engineering and Technology,Hyderabad, Andhra Pradesh, India*

Abstract:

The main purpose of this paper is to show some solutions for key management in mobile ad hoc networks. The major problem in providing security services in such infrastructure , how to manage the cryptographic keys that are needed. In order to design practical and sufficient key management systems it is necessary to understand the characteristics of ad hoc networks and why traditional key management systems cannot be used. The aim of key management is to provide secure methods for handling cryptographic keying algorithm. The tasks of key management includes keys for generation, distribution and maintenance. Key maintenance includes the procedures for key storage, key update, key revocation, etc. In MANETs, the computational load and complexity for key management are strongly subject to restriction by the node's available resources and the dynamic nature of network topology. A number of key management schemes have been proposed for MANETs.

Keywords: Wireless Security, Key Management Approaches, Key Management Scheme, MANETs.

1. Introduction

Ad hoc networking is a networking paradigm for mobile, self-organizing networks. Typically the network nodes are interconnected through wireless interfaces and unlike traditional networks lack specialized nodes, i.e. routers, that handle packet forwarding. Instead every node in the network functions as a router as well as an application node and forwards packets on behalf of other nodes. Ad hoc networks have the ability to form on the fly and dynamically handle the joining or leaving of nodes in the network. An example is when three people with ad hoc networking enabled PDAs come within communication range of each other. The three PDAs could then automatically create an ad hoc network used to exchange data.

The ad hoc networks generally presents the following characteristics :

Dynamic network topology: The network nodes are mobile and the topology of the network may change frequently. Nodes may move around within the network but the network can also be partitioned into multiple smaller networks or be merged with other networks.

Limited bandwidth: The use of wireless communication currently used implies a lower bandwidth than traditional networks. This may limit the number and size of the messages sent during protocol execution.

Energy constrained nodes: Nodes in ad hoc networks will most often rely on batteries as their power source. The use of complex algorithms, that consumes CPU time and energy there may not be possible.

Limited physical security: The use of wireless communication and the exposure of the network nodes increase the possibility of attacks against the network. Due to the mobility of the nodes the risk of them
being physically compromised by theft, loss or other means will probably be bigger than for traditional network nodes. By definition a mobile ad hoc network does not rely on any fixed infrastructure; instead, all networking functions (e.g., routing, mobility management, etc.) are performed by the nodes themselves in a self-organizing manner . For this reason, securing ad hoc networks is challenging and in some applications requires a shift in paradigms with respect to the traditional security solutions. The security is an important issue for ad hoc networks; one of the major problems in providing security services in ad hoc networks is how to manage the cryptographic keys that are needed. In order to design practical and efficient key management systems it is necessary to understand the characteristics of ad hoc networks and why traditional key management systems cannot be used. In this paper the main key management for ad hoc networks were reviewed and we proposed some solutions.

2. Key Management

As in any distributed system, in ad hoc networks the security is based on the use of a proper key management system. As ad hoc networks significantly vary from each other in many aspects, an environment-specific and efficient key management system is needed. The security in networking depends, in many cases, on proper key management. Key management consists of various services, of which each is vital for the security of the networking systems. The services

must provide solutions to be able to answer the following questions: Trust model, Cryptosystems, Key creation, Key storage and Key distribution.
The key management service must ensure that the generated keys are securely distributed to their owners. Any key that must be kept secret has to be distributed so that confidentiality, authenticity and integrity are not violated. For instance whenever symmetric keys are applied, both or all of the parties involved must receive the key securely. In public-key cryptography the key distribution mechanism must guarantee that private keys are delivered only to authorized parties. The distribution of public keys need not preserve confidentiality, but the integrity and authenticity of the keys must still be ensured. We showed some solutions for key management in ad hoc networks.

3. CHARACTERISTICS OF MOBILE AD HOC NETWORKS

It is important to acknowledge the properties or characteristics of mobile ad hoc networks (MANETs), since these properties can also be seen as *constraints* faced by researchers when designing security protocols for MANETs. Although these constraints are detailed in various articles and security protocols are frequently published that do not adhere to the fundamental design constraints. These constraints form the basis of protocol analysis. When a novel protocol or scheme is published for MANETs, the feasibility of the proposal is measured by (1) the degree to which the protocol satisfies the fundamental constraints of MANETs and (2) whether the protocol makes a justifiable tradeoff between security, memory requirements, and computational/communication overhead. Note that not all MANETs adhere to all of the characteristics detailed in this section.
The characteristics of MANETs and the possible applications are strongly related different applications demand MANETs with variants of the given characteristics. For example, an "open" or public MANET will take on a *self-organized* nature, and hence the end-users will set up and manage the network themselves. This means that an offline authority may not be available. In contrast, MANETs used in military applications will not have a self-organized characteristic, but will make use of an offline authority to initialize the nodes; the *authority-based* approach allows for robust access control to the network services.
Another example of varying characteristics emerges from MANETs formed by sensor nodes or laptop computers. Clearly schemes designed for MANETs formed by laptop computers will not have the same limitation on memory, energy (battery), and computational resources as those formed by sensor nodes.
It is thus apparent that a clear description of a key management scheme's intended application is necessary. The application may dictate the characteristics of the MANET and the degree to which some characteristics will influence the design of a suitable scheme.

4. APPLICATIONS OF MOBILE AD HOC NETWORKS

To understand the scope of MANETs and the usefulness of their unique characteristics, the potential applications of ad hoc networks are briefly considered. Ad hoc networks have applications in two major fields: military and commercial environments.

4.1. Military Applications

The origin of networks that rely on no preexisting infrastructure can be traced back to the early 1970s with the DARPA and PRNET projects, where the initial focus was on military applications. The application of ad hoc networks in a military environment is particularly attractive because of their lack of infrastructure and self-organizing nature. Consider conventional networks that rely on infrastructure such as base stations, the infrastructure introduces points of vulnerability which may be attacked and, if eliminated, dismantle the operation of the entire network. In battle field scenarios, robust and guaranteed communication is essential, with potentially fatal consequences if compromised. Ad hoc networks can continue to exist even in the event of nodes becoming disconnected due to poor wireless connectivity, nodes being compromised or switched off, nodes moving out of range, node being damaged during physical attack on users, or nodes failing due to malfunction or battery depletion. Applications such as sensor networks, positional communication systems and tactical ad hoc networks will continue to be some of the driving forces behind ad hoc network development.
The main characteristic of military-type MANETs is the use of an offline authority. In *authority-based* MANETs, nodes share pre-established relationships initialized by the offline authority. The presence or absence of a priori security relationships has a fundamental impact on the design strategy of key management schemes for MANETs.

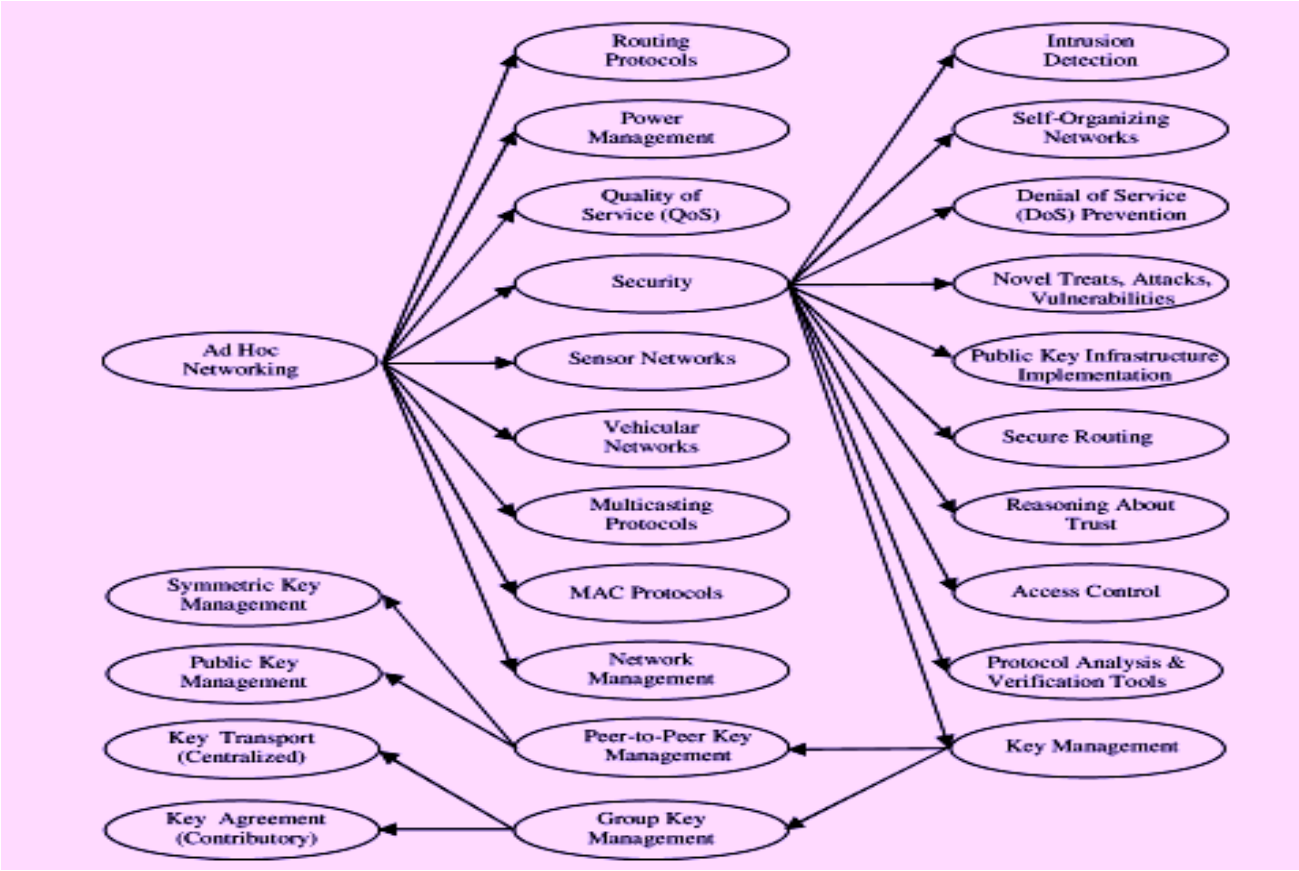
4.2. Commercial Applications

Commercial applications of ad hoc networks may include establishing connectivity in terrains where conventional networks, such as cellular networks, are not financially viable, cannot provide sufficient coverage, or need bypassing. Private networks or personal area networks (for the purpose of teleconferencing, video conferencing, peer-to-peer communications, ad hoc meetings, or, more generally,
collaborative applications of all kinds) are possible applications of ad hoc networks. It is anticipated that these applications will gain momentum as soon as the flexibility and convenience of self-organized ad hoc networking is fully appreciated and protocols are implemented with commercially available products. For example, cellular networks: what

was once seen as an impractical technology has now become a necessity. Emergency situations caused by geopolitical instability, natural, or man-made disaster could result in existing networking infrastructure being damaged or becoming unreliable. *Vehicular ad hoc networks* allow vehicles traveling along a highway to exchange data for traffic congestion monitoring, inter vehicle communications, and early warning of potential dangers ahead such as an accident, road obstruction, or stationary vehicle.

5. KEY MANAGEMENT IN MOBILE AD HOC NETWORKS

As an introduction to key management, this paper briefly considers the classification of security problems in MANETs. The aim is to position the problem of peer-to-peer key management within the MANET security field. The main observation is that cryptographic techniques are often at the center of solving security problems in MANETs and hence need key management . The subsequent subsections also provide definitions and terminology for the different properties and requirements of key management schemes.



5.1. Motivation for Key Management in Mobile Ad Hoc Networks

Despite the evolution of MANETs over the past decade, there are still a number of security-related problems that are open. It means that, although solutions have been proposed, none seems to satisfy all of the constraints of MANETs. Figure 1 illustrates the areas investigated within the MANET field, with particular focus on security issues. Note that this list highlights the main areas of ad hoc network security and could be expanded. As illustrated in Figure 1, research in the MANET security field is concerned with a variety of different aspects. Researchers in the ad hoc network security field initially focused on secure routing protocols. The focus of these protocols , SEAD , ARAN , SRP is twofold:

(i) To provide a routing mechanism that is robust against the dynamic network topology of MANETs.
(ii) To provide a routing mechanism that offers protection against malicious nodes.

Routing protocols may use various security mechanisms to mitigate attacks on the routing infrastructure. Some of these mechanisms are redundancy exploitation; diversity coding; on-demand route discovery; route maintenance techniques; fault- or intrusion-tolerant mechanisms, and cryptographic mechanisms. For example, routing schemes may exploit redundancy by establishing multiple routes from source to destination (as easily achieved by ZRP [Haas and Perlman 1998], DSR [Johnson and Maltz 1996], TORA [Park and Corson 1997], and AODV [Perkins and Belding-Royer 1999]) [Zhou and Haas 1999]. By sending data via all these routes, the redundancy will ensure that all data arrives at the destination. An alternative mechanism to sending data via redundant routes is *diversity coding* [Ayanoglu et al. 1993].

Diversity coding takes advantage of redundant routes in a more bandwidth-efficient way by not retransmitting the messages. Rather, it transmits limited redundant information through additional routes for the purpose of error detection and correction.
All of these mechanisms have various degrees of effectiveness. It is widely acknowledged that *cryptographic mechanisms* can provide some of the strongest techniques to ensure the availability, integrity, and confidentiality of routing information . This observation also holds true for many of the other MANET security problems highlighted in Figure 1 . If the basic networking mechanisms are considered, threat identification reveals that cryptographic techniques can also be used to mitigate attacks that exploit *over-the-air* communication, channel access mechanisms, and neighbor discovery.
Secure key management with a high-availability feature is at the center of providing network security via cryptographic mechanisms . However most routing schemes and related basic networking mechanisms neglect the crucial task of secure key management and assume preexistence and pre sharing of secret and/or private/ public key pairs. In fact, many cryptographic-based mechanisms that solve MANET security problems have a direct reliance on an efficient and secure key management infrastructure. This leaves key management techniques as an open research area in the ad hoc network security field.

5.2. Defining Key Management
A *keying relationship* is the state wherein network nodes share keying material for use in cryptographic mechanisms. The keying material can include public/private key pairs, secret keys, initialization parameters, and non-secret parameters supporting key management in various instances. Key management can be defined as a set of techniques and procedures supporting the establishment and maintenance of keying relationships between authorized parties. In summary, key management integrates techniques and procedures to establish a service supporting.

(1) initialization of system users within a network;
(2) generation, distribution, and installation of keying material;
(3) control over the use of keying material;
(4) update, revocation, and destruction of keying material;
(5) storage, backup/recovery, and archival of keying material, and
(6) bootstrapping and maintenance of trust in keying material.

Authentication is the basis of secure communication. Without a robust authentication mechanism in place, the remaining security goals (confidentiality, data integrity, and nonrepudiation) are in most instances not achievable. Authentication can only be realized by means of verifying something known to be associated with an identity. In the electronic domain, the owner of the identity must have a publicly verifiable secret associated with its identity; otherwise, the node can be impersonated. Authentication in general depends on the context of usage. Key management is concerned with the authenticity of the identities associated with the six services given above, it is a concept which may seem trivial at first, but one that is not easily achieved. Authentication of users is particularly difficult (and in most network settings impossible) without the help of a trusted authority.
The fundamental function of key management schemes is the establishment of keying material. *Key establishment* can be subdivided into key agreement and key transport . *Key agreement* allows two or more parties to derive shared keying material as a function of information contributed by, or associated with, each of the protocol participants, such that no party can predetermine the resulting value. In *key transport* protocols, one party creates or otherwise obtains keying material, and securely transfers it to the other party or parties. Both key agreement and key transport can be achieved using either symmetric or asymmetric techniques. A *hybrid* key establishment scheme makes use of both symmetric and asymmetric techniques in an attempt to exploit the advantages of both techniques.

5.3. Requirements of Key Management Schemes
Key management services should adhere to the following generic security attributes:

Confidentiality. Key management schemes should guarantee key secrecy, that is, ensure the inability of adversaries or unauthorized parties to learn keying material (or even partial keying material).

***Key authentication*.** Key authentication is a property whereby a communication entity is assured that only the specifically identified and authenticated communication entity may gain access to the cryptographic key material. Key authentication, in the context of a communication session between two parties, can either be *unilateral* or *mutual*: unilateral authentication means that only one party's keying material is authenticated, while mutual authentication involves validating both parties' keying material.
Possession of the key is in fact independent of key authentication. Key authentication, without knowledge that the intended recipient actually has the relevant key, is referred to as *implicit* key authentication.

Key confirmation. If key confirmation is provided by a key establishment protocol, communication entities prove possession of authenticated keying material. Key authentication with key confirmation yields *explicit* key authentication.

Key freshness. The *key freshness* property improves security by ensuring new and independent keys between different communication sessions. By separating communication sessions, the available information for cryptanalytic purposes is limited, which makes cryptanalytic attack more difficult.

Perfect forward secrecy. Perfect forward secrecy (PFS) ensures that compromise of *long-term* keys cannot result in compromise of past session keys.

Resistant to known key attacks. A key management scheme is vulnerable to *known key attacks* (KKA) if a compromised *past* session key or subset of past session keys allows the following:

(1) a *passive* adversary to compromise future session keys and (2) an *active* adversary to *impersonate* other protocol participants.

Forward secrecy. A key management scheme with a forward secrecy property prevents an adversary from discovering subsequent keys from a compromised contiguous subset of old keys.

Backward secrecy. A key management scheme with a backward secrecy property prevents an adversary from discovering preceding keys from a compromised contiguous subset of old keys.

Key independence. Key independence guarantees that a passive adversary who knows a proper subset of keys cannot discover any other keys. Key independence subsumes forward and backward secrecy. Key independence does not imply key freshness.

Availability. A high-availability feature prevents degradation of key management services and ensures that keying material is provided to nodes in the network when expected.

Robustness. The key management scheme should tolerate hardware and software failures, asymmetric and unidirectional links, and network fragmentation/partitioning due to limited/error prone wireless connectivity.

Survivability. Survivability is the capability of the key management service to remain available even in the presence of threats and failures. Survivability goes beyond security and fault tolerance to focus on the delivery of services, even when the system is partly compromised or experiences failures. (Survivability thus subsumes robustness.) Rapid recovery of services is required when conditions improve. Survivability includes *byzantine robustness*, which implies that the key management service should be able to function properly even if some misbehaving participating nodes attempt to disrupt its operation.

More specifically, key management services with a survivability feature focus on the delivery of essential services (for example certification services in public key infrastructure) and the preservation of keying material (public key certificates, session keys, etc.). Survivability can be summarized by the *The Three Rs*

Resistance: the capability of the system to defend against or tolerate attacks;
Recognition: the capability of the system to detect attacks in process and monitor the extent of the damage or compromise.
Recovery: the main feature of survivability; it is the capability to maintain services during attack, limit the extent of the damage and restore full services following the attack.
Efficiency. The key management service should be efficient with respect to communication, computational, memory, and energy resources.
Scalability. Scalability ensures efficiency and availability as the number of networking nodes rapidly and significantly changes; the key management scheme should thus seamlessly scale to network size.

6. PEER-TO-PEER KEY MANAGEMENT FOR MOBILE AD HOC NETWORKS

As mentioned in Section 1, the focus of this article is on peer-to-peer key management for mobile ad hoc networks (MANETs). Investigations by the authors within the available publications have led to the classification of the current protocols into the following subsets:
(1) partially distributed certificate authority;
(2) fully distributed certificate authority
(3) identity-based key management;

(4) certificate chaining-based key management;
(5) cluster-based key management;
(6) pre deployment-based key management;
(7) mobility-based key management, and
(8) parallel key management.
Most of the above subsets use public key cryptography due to its superiority in distributing keys, providing authentication, and achieving integrity and nonrepudiation. Symmetric key systems need a channel that provides both data integrity and confidentiality: the latter property may not always be readily available without any form of trusted authority or secure side channel (such as an infrared interface).

The *partially distributed certificate authority* group of protocols distributes the trust in the certificate authority to a subset of the network communication entities. The approach mitigates the single point of vulnerability inherent to the *centralized* certificate authority. Protocols considered to represent this implementation method were presented in Zhou and Haas [1999] and Yi and Kravets [2003], respectively. The *fully distributed certificate authority* protocol subset preserves the symmetric relationships between the communication entities in MANETs by distributing the burden of key management to *all* communication entities. Each authorized node in the network receives a share of the certificate authority's secret key, allowing neighbors to service requests for certification. The protocol that introduced this method was presented in Luo et al. [2002].

The *identity-based key management* approach borrows concepts from the *partially distributed certificate authority* protocols, but uses an identity-based cryptosystem to reduce the storage requirement compared to conventional public key cryptosystems. The protocol by Khalili et al. [2003] will be considered as representative of this protocol group.

In the *certificate chaining-based key management* approach, communication entities can authenticate certificates by means of finding certificate chains between them. Certificate chaining can be explained by the following example: party *A* wants to communicate with party *C*, which requires party *A* to authenticate party *C*'s certificate.

The two parties have no communication history, but party *A* trusts the certificate of a third entity, party *B*. Party *B* informs party *A* that it trusts the certificate of party *C*. Party *A* that trusts party *B* will thus also trust party *C* as a result of party *B*'s recommendation. There is thus a fully connected certificate chain between party *A* and *C* through party *B*, which enables party *A* to authenticate the certificate of party *C* without any previous communication.

The *cluster-based key management* subset relies on a clustering algorithm to subdivide the network into smaller groups. Group members in the same proximity can monitor their neighbors and make recommendations to members from other groups on the authenticity of their neighbors' certificates. The cluster-based subset is introduced by investigating the protocol presented in Ngai et al. [2004]. The *pre-deployment-based key management* subset makes use of an offline authority to issue each node with keying material prior to network formation. It is widely agreed that key pre-distribution techniques are ideally suited for establishing secure connectivity in large-scale distributed sensor networks [Eschenauer and Gligor 2002].

The limitations of sensor networks render conventional key establishment techniques (such as public key cryptography). The *mobility-based key management* subset exploits mobility and node encounters to establish security associations and to warrant mutual authentication between users. In contrast to the previously discussed subsets, the protocols in this group introduce a shift in paradigm with respect to previous attempts to provide key management for *fully* self-organized MANETs. Rather than trying to adapt solutions suited for conventional wireline networks, the protocols in this subset use the unique characteristics of MANETs to their advantage.

The combination of any of the above key management approaches gives rise to what the authors call the *parallel key management* subset. By using two or more of the above approaches in parallel, the advantages of the one scheme is used to mitigate the disadvantages of the other. This subset can be represented by the scheme introduced in Yi and Kravets [2004], which combines a *partially distributed certificate authority* [Yi and Kravets 2003] and the *certificate chaining-based key management approach* [Capkun et al. 2003b].

7. IDENTITY-BASED KEY MANAGEMENT APPROACHES

ID-based cryptography [Joye and Yen 1998; Boneh and Franklin [2001]; Cha and Cheon [2003] originated from the need to reduce the memory storage cost of conventional public key systems and the burden of obtaining explicitly authentic public keys. Public keys in an *ID*-based scheme are nothing other than the identities of the users themselves. The identities, which are publicly known data, must uniquely identify the users. *ID*-based schemes thus uniquely bind private keys to identities. The identity-based signature schemes are normally specified by four randomized algorithms [Boneh and Franklin 2001]:

(1) ***Setup***. The setup algorithm takes as input security parameters and returns a master public/private key pair *KM/kM* for the system. The master private key is only known by the trusted third party (TTP) or private key generator (PKG) of the system.

(2) ***Extract.*** The extract algorithm takes as input the master private key and an identity *ID* and returns the personal private key corresponding to the *ID*.

(3) ***Encrypt.*** The encrypt algorithm takes as input the master public key *KM*, the *ID* of the recipient, and a message *m* and returns the corresponding cipher text. Note that *ID* serves as the public key of the recipient.

(4) ***Decrypt.*** The decrypt algorithm takes as input the master public key, a cipher text, and the personal private key and returns the original message encrypted with the *ID* corresponding to the personal private key. The personal private keys in an identity-based cryptosystem can also be seen as an *implicit symmetric key certificate*, that is, the personal private key is encrypted with the master private key of the PKG.

8. CLUSTER-BASED KEY MANAGEMENT APPROACHES

The key management scheme proposed originates from the certificate chaining approach. The authors assumed a cluster-based network model constructed with the *zonal algorithm* [Chen and Liestman 2003]. The zonal algorithm for clustering ad hoc networks partitions the network into different subsets using a distributed algorithm for finding the minimum spanning tree (MST). Once the network is partitioned and the MST determined for each subset, the algorithm computes the weakly connected dominating sets of the regions. Finally, it fixes the borders of the clusters, that is, connects un-joined regions, by the inclusion of additional nodes in the sets. Nodes clustered together in the same region form a group and are assigned a unique *ID*. The nodes learn the group *ID*s of other nodes by exchanging messages.

9. PREDEPLOYMENT-BASED KEY MANAGEMENT

The limited memory, energy, and computational power of sensor nodes result from the constraints placed on their cost and physical dimensions. In uncontrolled deployment, which is normally the case with large-scale sensor networks, the nodes are randomly scattered over the target area. This implies an unpredictable network topology. Furthermore, sensors can be added and subtracted after deployment and may also encounter hostile networking environments. These characteristics result in key pre distribution being the only known, practical key establishment technique suitable for large-scale, wireless sensor networks.

10. MOBILITY-BASED KEY MANAGEMENT APPROACHES

Capkun et al. [2003a, 2006] proposed mobility-assisted key establishment schemes for MANETs. As mentioned before, the authors of this survey view these schemes as a significant advance in the state of the art: in contrast to the previously discussed subsets, the protocols in Capkun et al. [2003a, 2006] introduce a shift in paradigm with respect to previous attempts to provide key management for MANETs. Most of the existing key management schemes for MANETs try to modify solutions suited for conventional wireline networks which may not always be ideal in MANETs. The proposals investigated Capkun et al. [2003a, 2006] are peer-to-peer key establishment schemes that rely on user mobility to bring nodes within each other's transmission range. This allows them to exchange their keying material without relying on a secure routing infrastructure. This effectively breaks the routing-security interdependence cycle [Bobba et al. 2003]. The remainder of the section focuses on the key agreement techniques proposed in Capkun et al. [2003a, 2006] for *fully* self-organized MANETs.

11. PARALLEL KEY MANAGEMENT APPROACHES

Yi and Kravets [2004] proposed a multiple key management approach by combining a distributed certificate authority and certificate chaining. The proposal known as *composite* key management is based on two fundamental principles. First, key management should be shared between multiple nodes, and second, a trusted third party is required as an anchor of trust. Here certificates, as proposed in Capkun et al. [2003b], are stored and distributed by nodes in a self-organized nature. Yi and Kravets [2004] showed how a DCA can be used in *parallel* with certificate chaining to eliminate some of the weaknesses of the certificate chaining approach. The approach increases availability of the key management service since nodes can use either service to obtain keying material.

12. CONCLUSION

Key management schemes based on the key pre distribution techniques proposed for sensor networks may be another avenue to solve the key management problem in authority-based MANETs. Another observation is related to the criteria used by researchers to analyze key management schemes for MANETs. Key management schemes are designed either for an "open" (self-organized) or "closed" (authority-based) network and consequently aimed at different applications. "Open" or *fully* self-organized MANETs have some inherent security implications (such as being vulnerable against the Sybil attack [Douceur 2002]) and must be analyzed accordingly. It is therefore not always possible to compare schemes that assume the existence of a trusted authority with those that are fully self-organized.

This study confirms that key management mechanisms proposed to guarantee the security of conventional networks are not necessarily suitable or adaptable to MANETs. Novel techniques, designed specifically for MANETs, are necessary. Key management is an important area that will need resolution before wide-scale deployment of ad hoc networks will become practical. Although key management for MANETs has reached a reasonable level of maturity, it is still a research area with room for innovation.

References:

[1] JOHANN VAN DER MERWE, DAWOUD DAWOUD, and STEPHEN McDONALD, Peer-to-Peer Key Management for Mobile Ad Hoc Networks, ACM Computing Surveys, Vol. 39, No. 1,
[2] ABDUL-RAHMAN, A. AND HAILES, S. 1997. A distributed tust model. In Proceedings of the ACM New Security Paradigms Workshop.
[3] AKYILDIZ, I. F., SU, W., SANKARASUBRAMANIAM, Y., AND CAYIRCI. 2002. A survey on sensor networks. IEEE Commun. Mag. 40, 8 (Aug.), 102–114.
[4] ATENIESE, G., STEINER, M., AND TSUDIK, G. 1998. Authenticated group key agreement and friends. In Proceedings of the 5th ACM Conference on Computer and Communications Security.
[5] AYANOGLU, E., I, C.-L., GITLIN, R. D., AND MAZO, J. E. 1993. Diversity coding for transparent self-healing and fault-tolerant communication networks. IEEE Trans. Commun. 41, 11, 1677–1686.
[6] BETH, T., MALTE, B., AND BIRGIT, K. 1994. Valuation of trust in open networks. In Proceedings of the Third European Symposium on Research in Computer Security.
[7] BLOM, R. 1985. An optimal class of symmetric key generation systems. In Proceedings of EUROCRYPT'84.
[8] BOBBA, R. B., ESCHENAUER, L., GLIGOR, V. D., AND ARBAUGH, W. 2003. Bootstrapping security associations for routing in mobile ad-hoc networks. In Proceedings of the IEEE Global Telecommunications Conference.
[9] BONEH, D. AND FRANKLIN, M. 2001. Identity-based encryption from weil pairing. In Proceedings of the Conference on Advances in Cryptology (CRYPTO'01).
[10] BROCH, J. AND JOHNSON, D. B. 1999. The dynamic source routing protocol for mobile ad hoc networks. IETF Internet Draft. October.
[11] BUNDO, C., DE SANTIS, A., HERZBERG, A., KUTTEN, S., VACCARO, U., AND YUNG, M. 1993. Perfectly-secure key distribution for dynamic conferences. In Proceedings of CRYPTO'92.
[12] BUTTYAN, L. 2001. Building blocks for secure services: Authenticated key transport and rational exchange protocols. Ph.D. dissertation. Universite Technique de Budapest, Budapest, Hungary.
[13] BUTTYAN, L. AND HUBAUX, J. P. 2003. Stimulating cooperation in self-organizing mobile ad hoc networks. ACM Mobile Netw. Appl. 8, 5, 579–592.
[14] CAGALJ, M., CAPKUN, S., AND HUBAUX, J. 2006. Key agreement in peer-to-peer wireless networks. Proc. IEEE (Special Issue on Cryptography and Security) 94, 2, 467–478.
[15] CAPKUN, S., BUTTYAN, L., ANDHUBAUX, J.-P. 2003a. Mobility helps security in ad hoc networks. In Proceedings of MobiHoc.
[16] CAPKUN, S., BUTTYAN, L., AND HUBAUX, J.-P. 2003b. Self-organized public-key management for mobile ad hoc networks. IEEE Trans. Mobile Comput. 2, 1, 52–64.
[17] CAPKUN, S., HUBAUX, J., AND BUTTYAN, L. 2006. Mobility helps peer-to-peer security. IEEE Trans. Mobile Comput. 5, 1, 43–51.
[18] CARTER, C., YI, S., RATANCHANDANI, P., AND KRAVETS, R. 2003. Manycast: Exploring the space between anycast and multicast in ad hoc networks. In Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MOBICOM'03).
[19] CHA, J. C. AND CHEON, J. H. 2003. An identity-based signature from gap diffie-hellman groups. In Proceedings of the Conference on Public Key Cryptography (PKI'03).
[20] CHAN, A. C.-F. 2004. Distributed symmetric key management for mobile ad hoc networks. In Proceedings of the 23rd Conference of the IEEE Communications Society.
[21] CHAN, H. AND PERRIG, A. 2005. PIKE: Peer intermediaries for key establishment in sensor networks. In Proceedings of INFOCOM'05.
[22] CHAN, H., PERRIG, A., AND SONG, D. 2003. Random key predistribution schemes for sensor networks. In Proceedings of the IEEE Symposium of Privacy and Security.
[23] CHEN, Y. P. AND LIESTMAN, A. L. 2003. A zonal algorithm for clustering ad hoc networks. Int. J. Foundat. Comput. Sci. 14, 2, 305–322.
[24] CHRISTIANSON, B. 1996. Why isn't trust transitive. In Proceedings of the InternationalWorkshop on Security Protocols.
[25] DAHILL, B., LEVINE, E., ROYER, E., AND SHIELDS, C. 2001. A secure routing protocol for ad hoc networks. Tech. rep. UM-CS-2001-037. University of Massachusetts, Amherst, MA.

[26] DEARHAM, N. J. 2003. Development, implementation and quantification of an ad-hoc routing protocol for mobile handheld terminals. M. S. thesis in Electronic Engineering. Department of Electrical, Electronic and Computer Engineering, University of Natal, Durban, South Africa.
[27] DENG, H.,MUKHERJEE, A., AND AGRAWAL, D. P. 2004. Threshold and identity-based key management and authentication for wireless ad hoc networks. In *Proceedings of the International Conference on Information Technology: Coding and Computing* (ITCC'04).
[28] DESMEDT, Y. AND JAJODIA, S. 1997. Redistributing secret shares to new access structures and its applications. Tech. rep. ISSE-TR-97-01. Department of Information and Software Engineering, School of Information Technology and Engineering, George Mason University, Fairfax, VA.
[29] DOLEV, D. AND YAO, A. C. 1983. On the security of public key protocols. *IEEE Trans. Inform. Theor. 29*, 2, 198–208.
[30] DOUCEUR, J. R. 2002. The Sybil attack. In *Proceedings of the 1st International Workshop on Peer-to-Peer Systems* (IPTPS'02).
[31] DU, W., DENG, J., HAN, Y., CHEN, S., AND VARSHNEY, P. 2004. A key management scheme for wireless sensor networks using deployment knowledge. In *Proceedings of INFOCOM'04*.
[32] DU, W., DENG, J., HAN, Y. S., AND VARSHNEY, P. K. 2003. A pairwise key pre-distribution scheme for wireless sensor networks. In *Proceedings of the 10th ACMConference on Computer and Communications Security* (CCS).
[33] DU, W., DENG, J., HAN, Y. S., VARSHNEY, P. K., KATZ, J., AND KHALILI, A. 2005. A pairwise key pre-distribution scheme for wireless sensor networks. *ACM Trans. Inform. Syst. Secur. 8*, 2, 228–258.
[34] ESCHENAUER, L. AND GLIGOR, V. D. 2002. A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communication Security* (CCS'02).
[35] FEM 2005. U.S Federal Emergency Management Agency (FEMA): Information on federally declared disasters. Available online at http://www.fema.gov.
[36] FOUQUE, P.-A. AND STERN, J. 2001. One round threshold discrete-log key generation without private channels. In *Proceedings of the Public Key Cryptography* (PKC'01).
[37] FRANZ, W., EBERHARDT, R., AND LUCKENBACH, T. 2001. Fleenet—Internet on the road. In *Proceedings of the 8th World Congress on Intelligent Transport Systems*.
[38] GENNARO, R., JARECKI, S., KRAWCZYK, H., AND RABIN, T. 1999. Secure distributed key generation for discretelog based cryptosystems. In *Proceedings of the Conference on Advances in Cryptology* (EUROCRYPT'99).
[39] HAAS, Z. J., DENG, J., LIANG, B., PAPADIMITRATOS, P., AND SAJAMA, S. 2002. Wireless ad hoc networks. In *Encyclopedia of Telecommunications*, J. Proakis, Ed. John Wiley, New York, NY.
[40] HAAS, Z. J. AND PERLMAN, M. 1998. The performance of query control schemes for zone routing protocol. In *Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication* (SIGCOMM'98).
[41] HAAS, Z. J. AND TABRIZI, S. 1998. On some challenges and design choices in ad-hoc communications. In *Proceedings of the IEEE Military Communications Conference* (MILCOM'98).
[42] HERZBERG, A., JARACKI, S., KRAWCZYK, H., AND YUNG, M. 1995. Proactive secret sharing or: How to cope with perpetual leakage. In *Proceedings of the Conference on Advances in Cryptology* (CRYPTO'95).
[43] HU, Y.-C., JOHNSON, D. B., AND PERRIG, A. 2002a. Ariadne: A secure ondemand routing protocol for ad hoc networks. In *Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking* (Mobicom'02).
[44] HU, Y.-C., JOHNSON, D. B., AND PERRIG, A. 2002b. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. In *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications.*
[45] HUANG, D.,MEHTA, M.,MEDHI, D., AND HARN, L. 2004. Location-aware key management scheme for wireless sensor networks. In *Proceedings of the ACM Workshop on Security for Ad Hoc and Sensor Networks* (SASN).
[46] HUBAUX, J.-P., BUTTYAN, L., AND CAPKUN, S. 2001. The quest for security in mobile ad hoc networks. In *Proceedings of MobiHoc'01*.
[47] JOHNSON, D. B. AND MALTZ, D. A. 1996. Dynamic source routing in ad-hoc wireless networks. In *Mobile Computing*, T. Imielinski and H. Korth, Eds. Kluwer Academic Publishers, 153–181.
[48] JOSANG, A., GRAY, E., AND KINATEDER, M. 2003. Analyzing topologies of transitive trust. In *Proceedings of the First International Workshop on Formal Aspects in Security and Trust* (FAST'03).
[49] JOSHI, D., NAMUDURI, K., AND PENDSE, R. 2005. Secure, redundant, and fully distributed key management scheme for mobile ad hoc networks: An analysis. *EURASIP J. Wireless Commun. Netw.* 4, 579–589.
[50] JOYE, M. AND YEN, S.-M. 1998. ID-based secret-key cryptography. *ACM Operat. Syst. Rev. 32*, 4, 33–39.