Fully Distributed Authority-Based Key Management for Mobile Ad Hoc Networks

Dawoud S. Dawoud * and Johann van der Merwe

Dean of Engineering, Victoria University, Uganda
dawoud.shenouda@vu.ac.ug

Abstract
Securing wireless mobile ad hoc networks (MANETs) is challenging due to the lack of centralized authority and poor connectivity. Key management forms the basis for achieving many security objectives such as protecting routing protocols and private communications. We propose a novel key management scheme for MANETs that exploits mobility and the routing infrastructure to effectively manage security associations. Keying material propagates along virtual chains via a message relaying mechanism. We show that the proposed scheme results in a key management with low implementation complexity, ideally suited for stationary ad hoc networks and MANETs with low to high mobility. The proposed scheme uses mobility as an aid to fuel the rate of bootstrapping the routing security, but in contrast to existing schemes does not become dependent on mobility. The key dissemination occurs completely on-demand; security associations are only established, renewed or revoked as needed by the routing protocol and intrusion detection system. We show through simulations that the scheme's communication and computational overhead has negligible impact on network performance.

Index Terms
Mobile ad hoc networks, security, peer-to-peer key management, pairwise key management, authority based key management, network level key distribution, subordinate public keys

I. INTRODUCTION

Mobile ad hoc networks (MANETs) eliminate the need for pre-existing infrastructure by relying on the nodes to perform all network functions. The connectivity between the nodes is sporadic due to the shared, error-prone wireless medium and frequent link breakages caused by node mobility [1][2][3].
Many of the intended uses of MANETs require these systems to be appropriately secured [1]. For example, one of the well known applications of MANETs is vehicular communications [4] [5]. Without integrating security into vehicular networks (VNs), these systems may be compromised, jeopardizing the safety of the drivers and passengers. The consequences of not preventing abuse of VNs may even be fatal.
The characteristics of MANETs make them susceptible to numerous attacks and also challenging to secure. Key management is central to MANET security [1] [2] [6] [7] as most secure routing schemes [8] [9] [10] [11] neglect the crucial task of secure key management and assume pre-existence and pre-sharing of secret and/or public/private key pairs [1] [12].
The primary differentiation between existing peer-to-peer key management schemes can be based on the assumption of an off-line and/or on-line trusted authority [2] [6]. Key management schemes for MANETs can therefore be broadly grouped into *fully self-organized* schemes or *authority-based* schemes [2] [6] [3].
Authority-based MANETs address applications that demand the use of an off-line authority. The trusted authority sets up the nodes prior to network formation and may thus aid the nodes by providing strong access control to network services. In contrast to fully self-organized MANETs the nodes in authority-based MANETs do have pre-established relationships. Although authority-based MANETs are not formed purely *ad hoc*, they share the main characteristics of MANETs such as node mobility and lack of infrastructure. This paper expands the notion of authority-based MANETs [6] to also include MANETs that use a distributed *on-line* authority (in addition to the off-line authority). The distributed on-line authority may provide essential certification services such as certificate renewal and revocation.
The existing *authority-based* schemes are mostly *key pre-distribution* schemes [13] [14] [15] [16], ideally designed for sensor networks [3] (Vehicle Networks come under this group) . An off-line authority loads each sensor node with a large pool of keys prior to sensor deployment. The nodes then use this *a priori* distributed keying material to set up symmetric cryptographic keys between them during network formation.
Authority-based schemes that use public key cryptography normally combine an off-line authority with a distributed on-line authority. The schemes presented in [1] [17] [18] [7] are good examples of the offline and distributed on-line authority combination. These schemes, in contrast to the key pre-distribution schemes, are not designed for nodes with limited computational, memory and energy resources such as sensor networks. They can therefore take advantage of the benefits of public key cryptography such as efficient key distribution [1] [7] [19].

It is widely acknowledged that maintaining an on-line distributed certificate authority (DCA) is problematic in MANETs [2] [7] [3]. Luo *et al* [7] get around some of the DCA's main problems by forcing DCA servers to physically go back to the off-line authority to update their shares in the DCA's shared secret. In our point of view [7] still fails to eliminate the disadvantages of a DCA.

Capkun *et al* [6] proposes an *authority-based* scheme where each node is preloaded by the offline authority with a certificate. After network formation each node becomes its own authority domain and distributes its certificate to nodes within its transmission range. The scheme in [6] thus eliminate the problems associated with the DCA by completely eliminating the on-line authority altogether. The authority-based solution in [6] is mainly a mobility-assisted, *key distribution* scheme and do not provide all the required key management mechanisms such as certificate renewal and revocation (see Section-II for more details on [6] and [7]).

II. PROBLEM STATEMENT

Considering the discussion above on the existing key management schemes and by expanding on our problem statement in [20], we defined the problem as follows; the challenge is to design a straightforward authority-based *key management* scheme satisfying the following constraints:

- The key management scheme (including key generation, key distribution, key renewal and key revocation) must exploit mobility as originally shown by Capkun et al. [6], but in contrast to existing solutions [6] avoid relying on node mobility in any way; the key management mechanisms must therefore be fully functional in a stationary or low mobility ad hoc network and perform even better in a high mobility scenario. If the scheme is dependent on node mobility the key distribution mechanism will fail in low mobility or stationary settings which is the case in [6] [12].
- The scheme should be *fully distributed* and therefore equally share the responsibility of managing security associations between all nodes forming the network (during the entire lifecycle of the network). This is to ensure reliable security services that place the same burden on the computational, memory and energy resources of *all* nodes [1] [2].
- The key management scheme should break the *routing-security interdependence cycle* [21], while ensuring network scalability. Pre-distributing keying material to all the nodes, such that security associations between all nodes will be *guaranteed*, trivially mitigates the routing-security interdependence cycle. This however makes the network nonscalable; the offline trusted third party needs to engage with all nodes before the network can be formed. The management scheme should thus only require each node to be issued with its own keying material prior to network formation and not with the keying material of other nodes, that is, the scheme should allow for 'ad hoc' network formation.
- The scheme should avoid introducing any noticeable delay in the set up of security associations; the routing must be secure from the start of network formation, hence leave no window of opportunity for an attacker during security bootstrapping.
- The key management scheme should reduce communication and computational overhead to have negligible impact on network performance under realistic traffic and mobility scenarios.
- The scheme should avoid inflating the routing protocol control packets in order not to waste bandwidth.
- The key management scheme should introduce minimal changes in the underlying secure MANET routing protocol and integrate seamlessly with existing secure routing protocols as well as Intrusion Detection Systems suitable for MANETs.
- Certificates must be distributed (on-demand) as needed on the network (routing) layer and be transparent to the network participants, that is, the scheme should require no user involvement. Unnecessary user involvement makes the scheme prone to attacks that exploit human error.
- The offline authority essentially controls access to the network or limits use of the application to authorized users only. Examples of such networks include MANETs formed by users that serve a common purpose such as large scale emergency response operations and military missions. We assume that the offline authority may be compromised during the lifetime of the network, but this should not compromise the keying material of existing networking participants.

In this paper we focus on key management for authority-based MANETs given the constraints / requirements above. We expand on our preliminary work [3] [12] [20] and design a secure and efficient, authority-based public key management scheme called AuthBasedPKM. AuthBasedPKM consider mechanisms for public key generation, key distribution, key renewal and key revocation.

III. OVERVIEW OF PROPOSED SCHEME

AuthBasedPKM is broken down into an off-line phase and on-line phase.

1) AuthBasedPKM Off-line Phase: During the *off-line phase* each network participant (user) that wants to join the network must visit the off-line authority (network administrator) to obtain an authentic public/private key pair.

The user will physically take a node (networking device) to the authority for configuration. The configuration procedure is based on the authority-based public key establishment (APKE) protocol proposed in the paper. On completion of the APKE protocol, the node has the following: a universal set of system

parameters which includes the authentic public key of the off-line authority and an individual base public/private key pair. Note that the user is not issued with a conventional certificate by the offline authority but rather an implicitly authentic public key. The user's base public key can be implicitly authenticated using the off-line authority's public key.

Once the user has a base public/private key pair they generate a second or subordinate public/private key pair as presented by the authors in [12].

If a digital signature, generated by the user's subordinate private key, is also available then the legitimate user's base and subordinate public keys can be *explicitly* authenticated [3]. For this reason the user also generates a self-certificate using its subordinate private key to bind its identity to its subordinate public key. We will show that this binding also inherently holds between the user's identity and base public key.

AuthBasedPKM also make use of crypto-based identifiers [22] [23] to securely bound a nodes network address to the user's base public key.

Once the users have a unique subordinate public key the node can join the network and will be accepted by the other nodes as authorized to participate in the network if (and only if) the user's subordinate public key can be explicitly authenticated, i.e. if the user's certificate can be verified using the off-line authority's authentic public key.

2) AuthBased On-line Phase: The *on-line* phase of APKE involves key distribution, certificate renewal and certificate revocation. Since there is no form of (distributed) on-line authority whatsoever, all the key management functions are performed by the nodes in a fully distributed fashion. Similar to [6] [12] each node is its own authority domain, hence responsible for distributing certificates, updating its own subordinate public keys and keeping track of revoked certificates (invalid public keys). This feature effectively eliminates all the problem associated with a DCA as we describe in [3].

Key distribution is realized by our new scheme that exploits the routing protocol's control messages and uses intermediate nodes to relay public keying material along a virtual chain. The scheme, initially presented in [20], is called Certificate Dissemination based on Message Relaying (CertRelay). CertRelay provides key material on-demand to the routing infrastructure while breaking the classical routing-security interdependence cycle as described in [21].

The nodes use a self-organized key renewal procedure for deriving a new subordinate public key which is similar to the procedure that was used to generate the nodes' original subordinate public keys from the base public keys.

In [7] it is pointed out that key revocation is a common weakness in existing public key management schemes for MANETs. Most schemes realize revocation by relying on the nodes to proactively distributed their certificate revocation list (CRL) to other nodes. The proposed scheme, AuthBasedPKM, also makes use of CRLs but allow nodes to construct CRLs locally based on the output of a local (host-based) intrusion system. The new revocation scheme is also rooted in the characteristics of a suitable *distributed* intrusion detection mechanism for MANETs. If the node detects compromise of its keying material or the user suspect that its public key has been compromised the user implicitly distributed this information to the rest of the network using CertRelay.

III. PROPOSED AUTHORITY-BASED PUBLIC KEY ESTABLISHMENT SCHEME

The proposed authority-based public key establishment (APKE) protocol allows a single entity, party A, to negotiate for an authority-based public/private key pair (x_A, y_A) with a trusted third party, i.e. an *off-line* certification authority (CA). The new APKE scheme serves as a cryptographic building block in the off-line initialization phase of the proposed authority-based key management scheme (presented in Section-IV).

In this paper an APKE protocol is proposed that leverages the scheme proposed by Peterson *et al* [25]. The proposed APKE scheme is based on the modified ElGamal type signature variant, presented in [12]. The main motivation for proposing the new scheme is to improve on the security of [25], enhance its efficiency and to ensure compatibility with our preliminary work (subordinate public key renewal scheme) presented in [12].

The following system parameters and notations are applicable:

p, q two large primes, such that $q \mid (p-1)$.

g generator of the cyclic subgroup of order q in $(Z)_p^*$.

$H(\cdot)$ collision free one-way hash function.

x_P private key of party P.

y_P public key of party P, where $y_P = g^{x_P} \bmod p$.

To ensure the integrity of the data exchanged between the CA and party A a secure side channel is required such as an infrared interface or physical wire. The existence of such an authentic channel between party A and the CA is a reasonable assumption [7] [6].

It is assumed that the CA has a long-term base public/private key pair (x_{CA}, y_{CA}), generated by choosing a random number $x_{CA} \in_R [1, q-1]$ as its private key and a corresponding public key computed as $y_{CA} = g^{x_{CA}} \bmod p$.

The proposed protocol commence as follows:

1) The CA sends to party A the system parameters, p, q, g, $H(\cdot)$ and its public key y_{CA}.

2) Party A chooses random number $\bar{z}_A \in_R [1, q-1]$, computes $\bar{r}_A = g^{\bar{z}_A} \bmod p$ and transmits $\bar{r}_A$ to the CA.

3) The CA uses the modified ElGamal signature scheme presented in [12] to sign party A's certificate information KI_A. The CA chooses random number

$k_{CA} \in_R [1, q-1]$ and computes $r_{CA} = g^{k_{CA}}$ and $r_A = \bar{r}_A r_{CA} \bmod p$. The certification information for party A is set by the CA as $KI_A = [ID_A \| ID_{CA} \| r_A \| r_{CA} \| CertNo_{CA} \| IssueDate_{CA} \| ValPeriod_{CA} \| AddIn]$

Where ID_{CA} is the identity of the CA, $CertNo_{CA}$ a unique sequence number, $IssueDate_{CA}$ the date of issuing the certificate, $ValPeriod_{CA}$ the validity period and *AddIn* some additional extension information.

The CA must ensure that the user ID is unique. Note that the contents of KI_A can be altered based on the CA's certification policy. Inclusion of ID_A and r_A is however mandatory.

The CA computes the signature parameter,

$$s_{CA} = x_{CA} + H(KI_A)k_{CA} \bmod q, \quad (1)$$

and sends (s_{CA}, KI_A) to party A.

4) Party A can compute its private key as,

$$xA = s_{CA} + H(KI_A)\,\bar{k}_A = x_{CA} + H(KI_A)k_{CA} + H(KI_A)\,\bar{z}_A = x_{CA} + H(KI_A)[k_{CA} + \bar{z}_A] \bmod q \quad (2)$$

The triplet $(r_{CA}, \bar{r}_A, xA)$, can be seen as the proxy signature of the CA on KI_A. Party A verifies the signature of the CA and calculates the corresponding public key using Equation-3:

$$y_A \equiv g^{x_A} = y_{CA} \cdot y_{CA}^{H(KI_A)} = g^{x_{CA}} \cdot g^{H(KI_A)[k_{CA} + \bar{k}_A]} \bmod p \quad (3)$$

Section-V addresses the security and performance of the proposed APKE protocol.

IV. PROPOSED AUTHORITY-BASED KEY MANAGEMENT SCHEME

The proposed authority-based peer-to-peer key management scheme for MANETs, called AuthBasedPKM, will be presented next. We first discuss the system model and adversary model. Then we consider the *off-line* initialization phase, followed by the *on-line* post-initialization operation.

A. System Model

Similar to [2] [12] [26] [6], we consider a fully distributed network of wireless nodes with generic medium access control (MAC) and routing mechanisms. Nodes can be stationary or move with low to high mobility speeds ($0\text{m/s} - 20\text{m/s}$). We assume that there are no pre-existing infrastructure and no form of *on-line* trusted authority, hence our scheme does not make use of a distributed certificate authority as proposed in [1] [17] [18] [7]. The scheme requires an *off-line* trusted authority (TTP) to initialize the nodes prior to joining the network. This assumption is consistent with existing literature [1] [7] [6] and as noted in [7] allows for a high-level of protection to secure high-value communication in, for example, military type applications or in any MANET which requires strong access control.

Each node negotiates with the off-line TTP for a discrete logarithm, authority-based public/private key pair. The trusted authority thus only issues each node with their own key pair and not with the keying material of any other nodes. This is an important feature since it ensures scalability; the restriction avoids an impractical initialization phase for large-scale networks and allow new nodes to join the network at any point in time after network formation.

The base or originally generated key pair of users is never used for any real communication to protect it from attacks on the cryptographic algorithms used to secure communication. The users rather derive a second or subordinate public/private key pair from their base key pair. The notion of subordinate public key generation is presented in [12].

Each user then generates a self-certificate to bind other useful information to their keying material such as a unique sequence number, expiry date etc.

Any user with a valid self-certificate can join the network. After the initialization phase, each node becomes its own authority domain during network operation and is therefore responsible for the renewal, dissemination and revocation of its own certificates. In contrast to [12] that exchange certificates between nodes only on a peer-to-peer basis, our new key distribution mechanism distributes certificates using a peer-to-peer message relaying mechanism.

B. Adversary Model

We consider a straightforward general adversary model. An adversary is a malicious node that uses every means available to break the proposed key management scheme. Any *active* adversary can eavesdrop on all the communication between nodes, modify the content of messages and inject them back into the wireless channel. When a node is compromised all its public and private information is exposed to the adversary. In fact, the Dolev-Yao adversary model [27] is to restrictive [28], for example, it fails to capture information an adversary may gain from detailed knowledge of the protocols in use. We assume an active, *insider* adversary. The adversary can therefore make use of all the basic network services, such as the routing infrastructure.

The operation of AuthBasedPKM is divided into an *initialization phase* which is executed by each node and the trusted off-line authority before the user joins the network and a *post-initialization phase* which executes during network operation.

C. Initialization Phase of AuthBasedPKM

Each node Pi, for $(1 \leq i \leq n)$, contacts the off-line trusted authority for the system parameters and negotiates with the trusted authority for an authority-based base public/private key pair (x_i, y_i). The proposed authority-based public key establishment (APKE) protocol is detailed in Section-III.

Each node generates a unique identifier ($Address_i$) that is bound to its base public key yi as follows:

$$Address_i = H(y_i) \quad (4)$$

AuthBasedPKM requires Addressi to be used as the node's network address or as a fixed part of the address. Note that this requirement places no constraints on the structure of the network addresses: the entire hash

output, $Address_i$, can be used in MANETs with flat, static addresses or only a part of the output can be used in MANETs with dynamic addressing.

After each node established a public/private key pair (x_i, y_i) via the APKE protocol, each node P_i uses its base key pair to generate a subordinate public/private key pair (x_i', y_i') as follows [12]:

1) P_i chooses a random number $k_i' \in_R [1, q-1]$ and computes $r_i' = g^{k_i'} \bmod p$.

2) P_i computes its new subordinate private key as:

$$x_i' = x_i + H(KI_i \| r_i') k_i' \bmod q \qquad (5)$$

where KI_i is the original keying information supplied by the off-line TTP (see Section-III) and r_i' is P_i's public commitment.

3) Finally P_i computes its corresponding subordinate public key as:

$$y_i' = g^{x_i'} = y_i (r_i')^{H(KI_i \| r_i')} \bmod p \qquad (6)$$

To obtain an explicitly authentic key pair, P_i uses its newly obtained subordinate private key x_i' to sign its key information content, KI_i (concatenated with its subordinate public key y_i' and public commitment β_i' via the modified ElGamal signature scheme presented in [12]. Pi's certificate can then be defined as:

$Cert_i' = [KI_i \| y_i' \| CertNo_i \| IssueDate_i' \| ValPeriod_i' \| \alpha_i' \| \beta_i']$,

where (α_i', β_i') is the appended signature on ($(KI_i \| y_i' \| CertNo_i' \| IssueDate_i' \| ValPeriod_i' \| \beta_i')$

Note that Pi's base key pair (x_i, y_i) is never used for any real communication. Rather, each P_i uses its subordinate key pair (x_i', y_i') for securing actual communication.

D. Post-Initialization Phase of AuthBasedPKM

The post-initialization phase is defined from the start of network formation and involves mainly the following mechanisms:

1) Certificate distribution
2) Certificate authentication
3) Certificate renewal and revocation

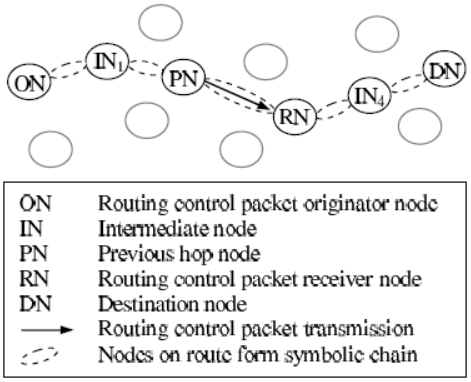
Here we introduce in a very short way the proposed certificate (key) distribution.

The details of the three mechanisms are given in a paper submitted to IEEE.

Proposed Key (Certificate) Distribution Scheme

The proposed scheme is designed specifically to have a low implementation complexity and to allow for easy integration into most secure MANET routing protocols. The proposed scheme, called Certificate Dissemination based on Message Relaying (CertRelay), is derived from the following straightforward procedure, illustrated in the next figure:

When a node (RN) receives a routing control packet it checks in its certificate database if it has the certificates of the packet originator (ON) and the previous-hop node (PN) on the forward route. If RN has both the certificates of ON and PN (CertON and CertPN), it can process the control packet as normal.



If not, it requests both the certificates from PN. If RN does not have the certificate of PN it also sends its own certificate with the request to the previous-hop. Note that if RN is the first-hop on the route, then the previous-hop node and the control packet originator node will be the same entity. The routing messages thus effectively chain nodes together and allow them to relay all keying material, as required, along the virtual chains.

The proposed key distribution scheme, CertRelay, is mainly based on the straightforward procedure introduced in Sect. I.

The scheme is summarized in Table I

TABLE I

MESSAGE EXCHANGE DECISION TABLE FOR RECEIVER NODE (RN)

Case 1: ON IP address = PN IP address			
Case#	ON cert stored	PN cert stored	Actions in sequence
1a	no	no	Peer-to-Peer certificate exchange $Cert_{RN} \longrightarrow ON$[a], $Cert_{ON} \longrightarrow RN$
1b	yes	yes	No action, process routing packet as normal
Case 2: Originator IP address ≠ PN IP address			
Case#	ON cert stored	PN cert stored	Actions in sequence
2a	no	no	Peer-to-Peer certificate exchange $[Cert_{RN} \| CertQ \longrightarrow PN]$[b] $[Cert_{PN} \| Cert_{ON} \longrightarrow RN]$
2b	yes	no	Peer-to-Peer certificate exchange $Cert_{RN} \longrightarrow PN$, $Cert_{PN} \longrightarrow RN$
2c	no	yes	$CertQ \longrightarrow PN$, $Cert_{ON} \longrightarrow RN$
2d	yes	yes	No action, process routing packet as normal

[a] RN = Receiver node, ON = Originator node, $Cert_X$ = certificate of X.

[b] PN = Previous-hop node, $CertQ$ = certificate query (RN uses this message to request $Cert_{ON}$ from PN, $A \| B$ = concatenation of messages A and B.

V. CONCLUSIONS

The proposed peer-to-peer key management scheme for MANETs, presented in Section-IV, makes use of authority-based public key establishment (introduced in Section-III), subordinate public keys [12] and crypto-based identifiers [22] [23] as building blocks to effectively eliminate the need for any form of on-line TTP. Constructing and maintaining an on-line TTP in MANETs has proven to be impractical.

The use a distributed certificate authority (DCA) as an on-line TTP makes the MANET vulnerable to attack

and eliminates a strong security argument. Our proposed scheme avoids these weaknesses by using a fully distributed system where each node becomes its own authority domain.

The complete analysis of the security of the proposed schemes are discussed in another paper submitted to IEEE.

REFERENCES

[1] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Network: special issue on network security*, vol. 13, no. 6, pp. 24–30, 1999.

[2] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-Organized Public-Key Management for Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, 2003.

[3] J. van der Merwe, D. Dawoud, and S. McDonald, "A Survey on Peer-to-Peer Key Management for Mobile Ad Hoc Networks," *ACM Computing Surveys (CSUR)*, vol. 39, no. 1, pp. 1–32, 2007.

[4] J.-P. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles," *IEEE Security & Privacy Magazine*, vol. 2, no. 3, pp. 49–55, 2004.

[5] M. Raya and J. P. Hubaux, "The Security of Vehicular Ad Hoc Networks," in *proc. ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'05)*, November, 7 2005, to appear.

[6] S. Capkun, J. Hubaux, and L. Buttyan, "Mobility Helps Peer-to-Peer Security," *IEEE Transactions on Mobile Computing*, vol. 5, no. 1, pp. 43–51, 2006.

[7] J. Luo, J.-P. Hubaux, and P. T. Eugster, "DICTATE: DIstributed CerTification Authority with probabilisTic frEshness for Ad Hoc Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 2, no. 4, pp. 311–323, 2005.

[8] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks," in *proc. Eighth ACM International Conf. on Mobile Computing and Networking (Mobicom'02)*, September 2002.

[9] ——, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *Workshop on Mobile Computing Systems and Applications. IEEE*, 2002.

[10] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad Hoc Networks," in *proc. SCS Communication Network and Distributed System Modeling and Simulation Conf. (CNDS'02)*, January, 27-31 2002.

[11] M. Guerrero Zapata, "Secure Ad Hoc On-demand Distance Vector (SAODV) Routing," September, 15 2005, iNTERNETDRAFT

[12] J. van der Merwe, D. Dawoud, and S. McDonald, "Fully Self-Organized Peer-to-Peer Key Management for Mobile Ad Hoc Networks," in *proc. ACM Workshop on Wireless Security (WiSe'05)*, September, 2 2005.

[13] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," in *proc. 9th ACM Conf. on Computer and Communication Security (ACM CCS'02)*, November, 17-21 2002.

[14] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Sensor Networks," in *proc. IEEE Symposium of Privacy and Security*, May, 11-14 2003.

[15] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 2, pp. 228–258, 2005.

[16] D. Liu, P. Ning, and L. Rongfang, "Establishing Pairwise Keys in Distributed Sensor Networks," *ACM Transactions on Information and System Security*, vol. 8, no. 1, pp. 41–77, 2005.

[17] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing Ad Hoc Wireless Networks," in *proc. Seventh International Symposium on Computers and Communications (ISCC'02)*, July 1-4 2002.

[18] S. Yi and R. Kravets, "MOCA: Mobile certificate authority for wireless ad hoc networks," in *proc. of the 2nd Annual PKI Research Workshop (PKI 2003)*, April, 28-29 2003.

[19] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook in Applied Cryptography*. CRC Press, 1996.

[20] J. van der Merwe, "Key Distribution in Mobile Ad Hoc Networks based on Message Relaying," in *proc. Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS'07)*, May, 22-25 2007.

[21] R. B. Bobba, L. Eschenauer, V. D. Gligor, and W. Arbaugh, "Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks," in *proc. IEEE Global Telecommunications Conference*, December 2003.

[22] G. O'Shea and M. Roe, "Child-proof authentication for MIPv6 (CAM)," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 2, pp. 4–8, 2001.

[23] G. Montenegro and C. Castelluccia, "Crypto-based Identifiers (CBIDs): Concepts and Applications," *ACM Transactions on Information and System Security*, vol. 7, no. 1, pp. 97–127, 2004.

[24] J. van der Merwe, D. Dawoud, and S. McDonald, "A Fully Distributed Proactively Secure Threshold-Multisignature Scheme," *IEEE Transactions on Parallel and Distributed Systems*, vol. 18, no. 4, pp. 562–575, 2007.

[25] H. Petersen and P. Horster, "Self-certified keys - Concepts and Application," in *proc. Third Conf. on Communication and Multimedia Security*, September 22-23 1997.

[26] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Mobility Helps Security in Ad Hoc Networks," in *proc. MobiHoc*, June 1-3. 2003.

[27] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[28] L. Buttyan, "Building Blocks for Secure Services: Authenticated Key Transport and Rational Exchange Protocols," Ph.D. dissertation, Universite Technique de Budapest, 2001.