THE CHALLEGES IN IMPLEMENTING SECURITY IN SPONTANEOUS AD HOC NETWORKS

Alastair Nisbet,
Security & Forensics Research Group
Auckland University of Technology
Auckland, New Zealand
anisbet@aut.ac.nz

Abstract

Mobile Ad Hoc Networks (MANETS) promise much in the ability to rapidly deploy a wireless network in a fashion where no prior planning is needed and the network can be running efficiently and with high security within minutes. Natural disaster response, military, education and business provide areas where MANETS can offer significant advantages in communication where infrastructure networks may take days to set up or may be impossible to implement. This research reviews a selection of MANET protocols to show the progression of the research and the issues that are yet to be addressed. It discusses the challenges to researchers in improving ad hoc schemes to the point where they work in theory and in practice. Areas are highlighted that pose the most significant challenges to developing new security protocols and some food-for-thought is given for those who wish to contribute to this growing area of importance for wireless communication.

Keywords - ad hoc networks, spontaneous, wireless, MANET, security, privacy, simulation

INTRODUCTION

In 1997 the Institute of Electrical and Electronics Engineers ratified the 802.11 wireless networking standard. Whilst wireless communications, including networking, had been available in various propriety applications for some years, the IEEE standard finally gave guidelines to manufacturers that allowed some interoperability of different vendor's equipment. This revolutionised wireless networking by bringing relatively cheap wireless devices to market that were not constrained to a single manufacturer. However, one serious drawback was that this original standard provided no built-in security. This left security to third party implementations which were seldom utilised by the users. In 1999, two supplementary additions to this standard resulted in IEEE 802.11a and 802.11b, providing much greater throughput. Whilst the benefits to throughput saw much greater uptake in the commercial and private sector, it was the inclusion of security in the form of Wired Equivalent Privacy (WEP) that offered considerable benefits. This security utilised the RC4 symmetric stream cypher and provided for up to 4 different encryption keys that could be paired between a user and a wireless access point. The ability to require the entering of an encryption key for a potential user to join the network provided significant security. Issues with the security of WEP were fairly quickly identified (Fluhrer, Mantin et al. 2001) and proved shortly afterward with a practical implementation of the attack (Stubblefield, Ioannidis et al. 2002). However, the introduction of WPA in 2003 and other security protocols 'fixed' these known problems and this led to a much greater uptake of the technology (Lashkari, Danesh et al. 2009). Not only were the messages between communicating parties now secured with a robust encryption algorithm, but unauthorised users could be prevented from joining the network by simply keeping the encryption keys secret. One further benefit was that users who were previously authorised and provided with the key, could be simply excluded once their authorisation expired by changing or deleting the key on the access point. The ability to allow only authorised users on a network is a prime requirement for a secure network but also highly desirable for the home user who does not want his messages read by unauthorised eavesdroppers and does not wish to provide free Internet connectivity to his neighbours.

The ability to form a network utilising one or more access points provides a simple setup of a network within a commercial or private setting. However, whilst this infrastructure mode is the most common, the ability for users to connect directly to each other wirelessly without an access point provides greater scope for utilisation of a network. This 'ad hoc' mode has taken some time to gain acceptance, but as time has passed greater and greater benefits have been envisioned. These benefits may be in military, commercial or educational setting and

one area that is currently being explored is that of disaster relief and recovery. Whatever the setting, one feature that is always of benefit is providing security. The ability to communicate privately or to ensure only authorised and well-behaving users are utilising the network is often of primary importance. Whilst the idea of security using well-established algorithms seems simple, in an ad hoc setting where no access points exist to maintain control over the network makes this type of topology extremely challenging for implementations of security. The following section looks at a selection of proposed MANET protocols. These identify the various approaches research has taken as time has gone by and show the progression of ideas in the development of the various schemes.

LITERATURE REVIEW

MANET development has existed in various forms for several decades but as with all wireless networking, it did not see any significant uptake amongst home and commercial users until the suite of IEEE 802.11 protocols were ratified beginning in 1997. The following MANET schemes are examined to highlight the issues with developing these protocols and the various approaches that have been undertaken.

The MOCA (Mobile Certificate Authority) protocol was an early scheme developed for pre-planned MANETS (Yi and Kravets 2003). Specifically utilising the mobility of some nodes in the network to provide certificate authorities (CAs) that moved throughout the network was something of a novel approach. The MOCA protocol realised the benefits of Public Key Infrastructure (PKI) to gain some control over the users of the networks and utilised pre-installed digital certificates in all nodes that would form the network. The heterogeneous nature of the nodes meant that more robust or powerful nodes could be chosen to collectively make up the certificate authority by combining to produce information that would be sent to the certificate requestor. This use of threshold cryptography greatly increased resilience to a successful attack against one or more CA nodes. The requestor could then combine the information to construct the certificate, keeping the private key secret in the process. This protocol also identified the need for redundancy of CA nodes by permitting more CA nodes in the network than was required. This was expressed as:

$$M > n > k$$

Here M is the total number of nodes in the network, n is the total number of CA nodes and k is the number of CA nodes that are required to combine to provide the certificate service. MOCA provides a high level of security with fault tolerance meaning the CA is considerably more likely to be available at all times and at least one CA node should be within a short distance of a node checking another node's certificate status. The retaining of certificate information in all CA nodes is a priority if the ability to revoke certificates of misbehaving or compromised nodes may be required. The drawbacks with MOCA are that it will only work with pre-configured nodes and is designed for one single network. It does not deal with networks that combine and split into smaller networks and it allows a single CA to revoke a certificate. This is something that should only be done if all CA nodes are entirely trustworthy.

The SKYE (Secure Key deploYment and Exchange) protocol is designed for a spontaneous network (Nisbet and Rashid 2009). The challenge for this protocol was to allow any node to join the network yet provide privacy and robustness against misbehaviour. This protocol utilised some of the features of MOCA but had significant modification to provide for a truly spontaneous deployment. SKYE was developed by examining many other schemes that existed and selecting those features that should be utilised if possible and identifying those that should be avoided. Several further unique features were then added.

PKI provides more robust resilience to attacks on secret or private keys than symmetric key protocols because an attacker gaining knowledge of one secret PKI key in a conversation will only gain the ability to listen to one side of a conversation. The attacker must compromise both private keys to decrypt the entire conversation. However, PKI usually requires regular contact with the CA and therefore greater overhead of communications meaning less time for other messages and draining battery life of devices more quickly. This may not always be

the case if schemes utilise PKI without a CA such as AC-PKI (Zhang, Liu et al. 2005). However simplified this may be a lack of CA requires trust in all nodes, something that is not possible in a spontaneous network.

The SKYE protocol demanded joining nodes to begin their communications with PKI and request a digital certificate from the closest CA node who then contacted *k*-1 nodes. These other CA nodes forwarded their parts of the certificate to the first node who forwarded all parts to the requester. This placed the burden of contacting the additional CA nodes on the CA itself, enhancing security and efficiency by placing more control in the hands of the CA than MOCA.

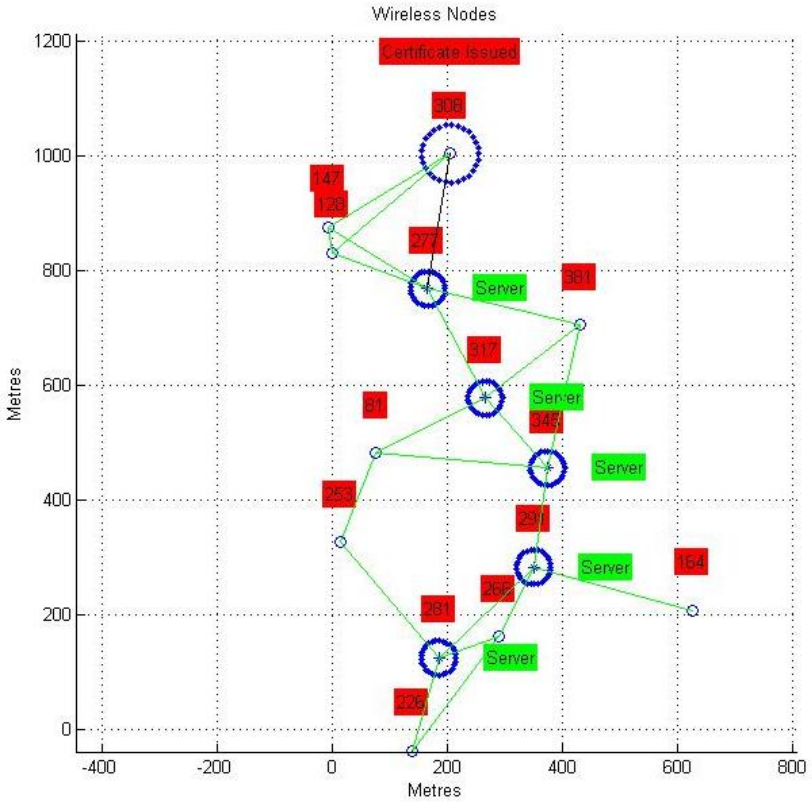

Figure 1: Example of SKYE Protocol Certificate Request

Figure 1 shows node 308 at the top of the grid requesting a certificate from the closest server, node 277. In this example, $k = 5$. Server node 277 then takes control by contacting the other 4 required servers. Each request is treated separately, so a message is sent to the closest sever to 277 which is 317. This node replies to 277 with certificate information. Server 277 then contacts the next closest server, 345. This server replies to 277 and so on until server 277 has all 5 parts of the certificate information. The server then sends all 5 to the requesting node who calculates the certificate including the private and public key pair. In this example, 22 hops are required before node 308 has all the information required. In the MOCA protocol, node 308 as the certificate requester would take responsibility for contacting all 5 servers. This will require 31 hops to receive all 5 responses. This is both less efficient and places more trust in the requesting to node to legitimately contact all 5 required servers rather than in a more trusted server.

Additionally, the SKYE protocol required *k* CA nodes to combine to eject a node after receiving a threshold of complaints about a node in a selectable time frame. Whilst there may be regular message exchanges between CA nodes in the network to provide up-to-date management, the extra overhead is offset by the increased security. This meant that several CA nodes would effectively vote a node out of the network providing robustness against a misbehaving CA node. Simulations showed that often several independent networks would form and with mobility of some nodes these networks would join to form bigger networks or split into smaller networks. This point is important because often researchers assume a spontaneous network will form and nodes

will join this single network. In many applications this may not be the case. Several networks may begin independently, only joining through growth or mobility. Figure 2 shows a simulation of a spontaneous network growing over time from a single node. The left simulation grid shows the various network formations after 300 seconds of growth whilst the right grid shows the same network after 600 seconds. The figure shows how initially several independent networks may form whilst the right figure shows how growth may lead to a joining of all networks into one large network. The circles indicate the 300 metre radio range of isolated nodes. Green indicates no certificates issued while red labels indicate a successful certificate issuance to the node.

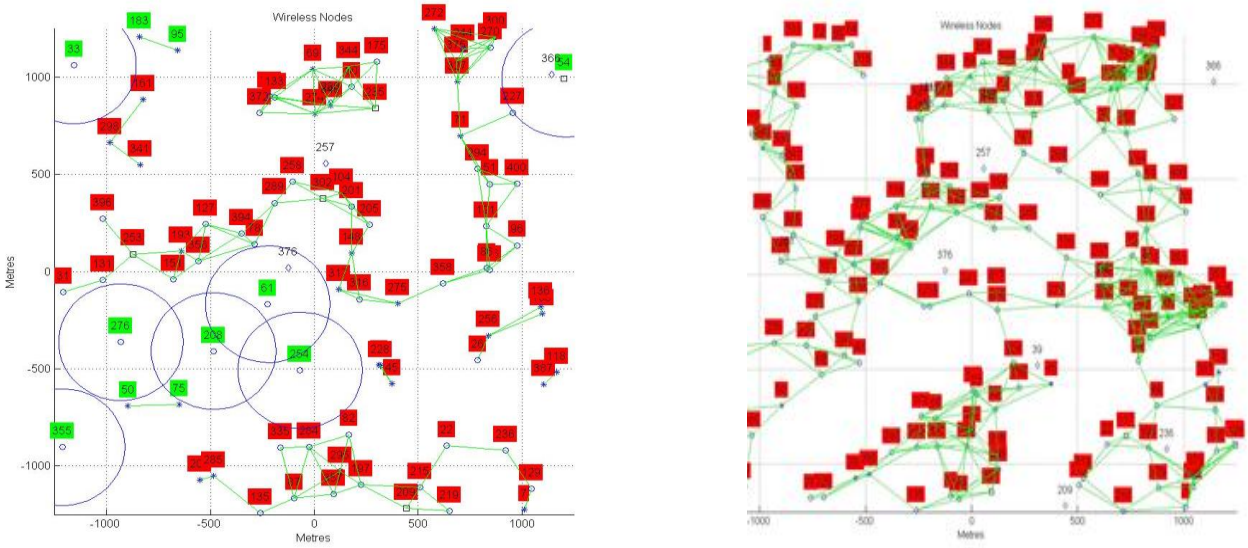

Figure 2: Simulation of Spontaneous Network Growth

One feature MOCA and SKYE had in common is utilising threshold cryptography where at least 2 nodes must have their knowledge combined to create a digital certificate with public / private key pairs. The prospect of being able to tune the parameters such as *n*, *k*, and in the case of SKYE the complaints received and the timeframe required for complaints, meant for a particular implementation there are significant benefits by making these protocols suit different types of implementations where security versus efficiency may lend itself to a trade-off between the two. In some cases, the protocols can fine tune these parameters as the network grows, maintaining efficiency in increasingly demanding situations.

Some schemes take the approach of dividing the large security problem into smaller problems. These cluster schemes split the network into logical clusters and identify each cluster as a separate network. They then provide a method for inter-cluster communication. This idea was first proposed in 1999 (Basagni 1999). A later scheme provided this method and included authentication of the nodes (Gomathi and Parvathavarthini 2010). These schemes usually utilise a group leader to provide security, but one scheme proposed a cluster-based approach utilising threshold cryptography without a leader (Noack and Spitz 2009). This fits more with a spontaneous formation where selecting group leaders who are unfamiliar may be an undesirable risk.

More recently, the idea of spontaneous wireless networks has gained interest with later schemes often considering the level of security required for a particular application. One such scheme considered the adaptive nature required for the nodes in the network based on energy constraints, node variability and bandwidth limitations (Lacuesta, Lloret et al. 2013). This awareness of adaptability for nodes and the network in general is a progression of the tuneability criteria identified over a decade before. In this research, criticisms of the lack of previous research fully considering security are made and this point highlights the continued need for a fully developed protocol with practical possibilities.

One protocol recently revised the idea of utilising symmetric key encryption but the focus was on simplicity and preservation of resources rather than robust security (Jegatheesan and Manimegalai 2014). Whilst symmetric

encryption may be a suitable level of security for many applications, the exchange of the shared key will generally require Diffie-Hellman Key Exchange. One such scheme proposed symmetric keys for all communications utilising Diffie-Hellman for the exchange. Something that was proposed early on in ad hoc research and highlights the need for building on previous research rather than restating what has come before (Taneja, Kush et al. 2011).

The idea of developing a hierarchical scheme for spontaneous networks was postulated in 2001 (Yang and Zheng 2001). This idea was developed in 2006 (Wang and Fang 2006) and the following year (Wang and Fang 2007) but hierarchical scheme development has fallen out of favour due the issues with developing a hierarchy spontaneously. However, this type of topology does fit well with routing protocols and this is one area that could see revival in the future, especially if permanently and uniquely identifying nodes is possible.

This review of previous schemes is a selection of the more well-known schemes developed over the previous 2 decades. The progression of ideas can be seen but the mix of disjoint ideas is also clear. This is perhaps one reason that no single scheme is seen as fit for purpose for a variety of applications.

DISCUSSION

The challenge to security within a MANET primarily arises from the lack of a centre of control. The issue arises when a network is available to all prospective users, yet the ability to control the use of those who join the network is a necessity. In a spontaneous network where no user is superior to any other user, the ability to restrict use and eject misbehaving users is a significant challenge. One problem with designating a node to implement security is that there is an equal chance that the designated node may be trusted or is a malicious node. Designating authority over the network could then become a disaster from its very beginning. The pre-installation of certificates is a simple step to ensuring digital certificates are created and stored securely in nodes and the CA, but this is not possible in a spontaneous MANET.
Some of the challenges that remain for truly ad hoc MANETS and areas that require further research are as follows:

1: Providing for symmetric key encryption only requires either a single key for the network or key pairs for every node in the network with every other node. The first option provides no security from other nodes with the key and means constant rekeying is required if nodes are ejected. The second option creates significant traffic with key exchange, where either a node joining the network will take an active approach and exchange unique keys with every other node in the network, or will wait until communication is requested to exchange keys. The former creates overwhelming key exchange and could significantly disrupt the network with key exchange messages. The latter is a better approach but still allows for fairly simple attacks against the keys such as Man in The Middle (MTM) attacks by rogue nodes.

2: Networks that combine with other networks or split apart may require new keys so that security can be maintained. If PKI is utilised, how can a CA be sure that its certificate repository is always up to date with current and revoked certificates?

3: Choosing a CA node on-the-fly means there is an unavoidable risk of making a malicious node a CA. Whilst PKI makes ejection of a node fairly straightforward, such as when complaints about a misbehaving node are made to the CA, how can the CA nodes be sure that the complaints are genuine? They may be made by a rogue CA node or a malicious node.

4: Threshold cryptography provides greater security by dividing the knowledge between nodes. However, if the CA nodes required (k) are not yet available in an establishing network, certificates cannot be obtained For example, 20% of nodes designated as CA nodes is common in these schemes. If k is 5, then there must be at least 25 nodes in the network before there will be 5 CA nodes. This would require waiting without communication until there are sufficient nodes, or in the case of SKYE, overriding the rule until sufficient nodes exist. In this example, SKYE would designate the first 5 nodes in the network as CA nodes so that communication begins when just 5 nodes are online. No other CA node will be designated until 30 nodes are in

the network. Overriding rules may be necessary with the design of the protocol to allow communications early on, but overriding security rules is highly undesirable.

5: Complaints of misbehaviour are difficult to verify. Firstly, defining misbehaviour is difficult. Secondly, false positives for misbehaviour may be commonplace where communication could be disrupted by interference or nodes forced temporarily offline. Allowing for a threshold of misbehaviour may be required but defining misbehaviour and providing a realistic threshold that does not permit a level of genuine misbehaviour is difficult.

6: A significant area of required research exists in identifying forensic evidence from MANETS. Nodes may all be unknown to each other and reconstructing events to identify serious misbehaviour that may have resulted in criminal actions is almost impossible. This requires identities to be bound to nodes and the ability to construct evidence when only a small section of nodes may be available for examination.

7: The ability to uniquely and permanently identify a node is crucial. Whilst this problem was identified over 30 years ago, this problem has yet to be solved (Shamir 1984). Recent research has identified this as crucial for spontaneous networks (Saini, Shukla et al. 2014). This is required to prevent a Sybil attack where a node may take on more than one identity (Douceur 2002). This can also lead to Byzantine behaviour where several nodes collude to disrupt the network. If a node's identity can be easily changed by the node, then ejecting misbehaving nodes does not solve the problem.

8: Many new schemes published bolster their proposals by criticising other schemes. However, many criticisms are unfounded and show a lack of understanding of the protocols. For example, one report criticised SKYE for not being scalable when one of the significant benefits of this scheme is that it is simply and efficiently scalable to any size. Developers of new schemes may blindly accept these criticisms without themselves understanding how the scheme works. Researchers must fully understand the problems with MANET security and what has been developed and only then make criticisms. They must then build on the knowledge rather than creating disjoint schemes that thus far all have drawbacks.

9: If PKI and CA nodes are utilised, then the location of those nodes has a significant impact on efficiency. Much research is still required on how best to select CA nodes, particularly with regards to their relative locations in the network (Nisbet, Rashid et al. 2010).

10. When modelling mobility of nodes in a simulation of a MANET, the correct number of mobile nodes, their direction and their speed is often 'best guess' rather than realistic (Theoleyre, Tout et al. 2007). For example, the Random Waypoint Mobility Model is common for modelling people walking but requires the mobile node to head to a random point, then head to another random point and so on, all the while remaining in the simulation area. Clearly this is not realistic. Other mobility models are sometimes used, but no model so far truly mimics realistic travellers (Ariyakhajorn, Wannawilai et al. 2006; Theoleyre, Tout et al. 2007).

11: The ideal for researchers is to develop one single scheme that can be utilised for many different uses. The best approach would seem to be providing tuneability to the various attributes of the scheme as has been seen in schemes such as MOCA and SKYE.

12: MANET research requires emersion by the researchers to fully appreciate the difficulties and design solutions. This is not a suitable area to research as an offshoot of network security that may be seen as a trendy, short-lived diversion.

CONCLUSION

MANET security is a significant and on-going challenge for researchers. Whilst there have been many MANET security schemes developed, they range from unrealistic or insecure, to compromises that provide good security but with overwhelming overheads. The challenge is to find the balance of security robustness versus efficiency within the network. Whilst more management messages, especially broadcast messages, make sustaining the network simpler, they may have such a significant impact on the effectiveness of the network that the protocol

does not translate from theory to practice. What is needed to improve MANET protocols to where they become commonplace is significant and dedicated research from people who are willing to put their research efforts into this small but highly significant area. There will a time when MANETS can be deployed in a spontaneous fashion and be both secure and efficient, but the time that it takes to get to this point will be determined by the efforts that are made to fully understand previous research and to build on this with new and innovative ideas.

REFERENCES

Ariyakhajorn, J., P. Wannawilai, et al. (2006). A Comparative Study of Random Waypoint and Gauss-Markov Mobility Models in the Performance Evaluation of MANET. International Symposium on Communications and Information Technologies, 2006. ISCIT '06.

Basagni, S. (1999). Distributed clustering for ad hoc networks. Fourth International Symposium on Parallel Architectures, Algorithms and Networks, Perth, Western Australia.

Douceur, J. R. (2002). The Sybil Attack. Revised Papers from the First International Workshop on Peer-to-Peer Systems, Springer-Verlag.

Fluhrer, S., I. Mantin, et al. (2001). Weaknesses in the key scheduling algorithm of RC4. Eighth Annual Workshop on Selected Areas in Cryptography. Toronto, Canada.

Gomathi, K. and B. Parvathavarthini (2010). An Efficient Cluster Based Key Management Scheme for MANET with Authentication. Trendz in Information Sciences & Computing (TISC), IEEE.

Jegatheesan, A. and D. Manimegalai (2014). "Symmetric key management for mobile ad hoc networks using novel secure and authenticated key distribution protocol-revised " International Journal of Electronic Security and Digital Forensics 6(4): 268-284.

Lacuesta, R., J. Lloret, et al. (2013). "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation." IEEE Transactions on Parallel and Distributed Systems 24(4): 629-641.

Lashkari, A. H., M. M. S. Danesh, et al. (2009). A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). 2nd IEEE International Conference on Computer Science and Information Technology, 2009. ICCSIT 2009. .

Nisbet, A. and M. A. Rashid (2009). A Scalable and Tunable Encryption Key Management Scheme for Mobile Ad Hoc Networks. International Conference on Wireless Networks 2009, Las Vegas, NV.

Nisbet, A., M. A. Rashid, et al. (2010). The quest for optimum server location selection in mobile ad hoc networks utilising threshold cryptography. 7th International Conference on Information Technology - New Generations. Las Vegas, USA: 891-896.

Noack, A. and S. Spitz (2009). "Dynamic Threshold Cryptosystem without Group Manager." Network Protocols and Algorithms 1(1).

Saini, S., A. Shukla, et al. (2014). "A Survey of Security in Mobile Ad-Hoc Networks using Cryptography." International Journal of Advanced Research in Computer Science and Software Engineering 4(10): 193-200.

Shamir, A. (1984). Identity-Based Cryptosystems and Signature Schemes. Crypto '84, Santa Barbara CA.

Stubblefield, A., J. Ioannidis, et al. (2002). Using the Fluhrer, Mantin, and Shamir attack to break WEP. Network and Distributed Systems Security Symposium (2002).

Taneja, S., A. Kush, et al. (2011). Secret Key Establishment for Symmetric Encryption over Adhoc Networks. World Congress on Engineering and Computer Science, San Francisco, USA.

Theoleyre, F., R. Tout, et al. (2007). New metrics to evaluate mobility models properties. 2nd International Symposium on Wireless Pervasive Computing, 2007. ISWPC '07.

Wang, N.-C. and S.-Z. Fang (2006). "A Hierarchical Key Management Scheme for Secure Group Communications in Mobile Ad Hoc Networks." The Journal of Systems and Software 80: 1667-1677.

Wang, N.-C. and S.-Z. Fang (2007). "A hierarchical key management scheme for secure group communications in mobile ad hoc networks." Journal of Systems and Software 80(10): 1667-1677.

Yang, P. and S. Zheng (2001). Security management in hierarchical ad hoc network International Conferences on Info-tech and Info-net, Beijing, China.

Yi, S. and R. Kravets (2003). MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks. Annual PKI Research Workshop Program, Maryland, USA.

Zhang, Y., W. Liu, et al. (2005). AC-PKI: Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks. IEEE International Conference on Communications. IEEE. Seoul, Korea.