

Dynamic trust establishment in emergency ad hoc networks

Christos Papageorgiou,
Konstantinos Birkos
Dept. of Electrical and
Computer Engineering
University of Patras, Greece
xpapageo@ceid.upatras.gr
kmpirkos@ece.upatras.gr

Tasos Dagiuklas
Dept. of Telecommunications,
Systems and Networks
TEI of Mesolonghi
Nafpaktos, Greece
ntan@teimes.gr

Stavros Kotsopoulos
Dept. of Electrical and
Computer Engineering
University of Patras, Greece
kotsop@ece.upatras.gr

ABSTRACT

This paper proposes a dynamic trust establishment protocol that enables the nodes of an ad hoc network to establish security associations among each other in a distributed and peer-to-peer manner. The basis of the protocol is a node-to-node security handshake using a network-wide key that every node is preconfigured with. This way a security association is established between the involved nodes. The information regarding such an association is propagated to the rest of the trusted nodes, resulting in the formation of a secure network overlay. The protocol is dynamic in the sense that the nodes keying material is periodically renewed by a set of leader nodes in order to enhance the system security. Although generic, our protocol is best suited to emergency ad hoc networks, where the aforementioned assumptions about the node preconfiguration and the reliability of the leader nodes are applicable. The proposed protocol extends previous work on authority-based trust establishment schemes by using a renewal process of the nodes' keying material and by being independent of the underlying routing protocol and the nodes' communication capabilities. Simulation results show that the performance of the protocol depends directly on the network connectivity, the number of leader nodes and the node mobility level.

Categories and Subject Descriptors

C.2.0 [General]: Security and protection; C.2.1 [Network Architecture and Design]: Network communications

General Terms

Algorithms, Experimentation, Performance, Security

Keywords

wireless, ad hoc, networks, trust establishment, renewal

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

IWCMC '09, June 21-24, 2009, Leipzig, Germany.

Copyright 2009 ACM 978-1-60558-569-7/09/06 ...\$5.00.

1. INTRODUCTION

The unique characteristics of the ad hoc networks make them the only feasible solution for communication in many cases, with emergency situations being a primary example. Security in these networks is far more challenging than in the wireline networks due to the broadcast nature of the wireless medium and the frequent topology changes, while its importance is fundamental given that their application range covers sensitive scenarios. Trust establishment, as part of a complete security solution covering all layers of operation of an ad hoc network, provides the means to secure both the routing process and the applications intended to be performed in the network.

In this work, we propose a trust establishment protocol that enables the nodes of an ad hoc network to establish security associations among each other in a distributed and peer-to-peer manner. The basis of the protocol is a node-to-node security handshake using a network-wide key that every node is preconfigured with. The information regarding such an association is propagated to the rest of the trusted nodes, resulting in the formation of a secure network overlay. The protocol is dynamic in the sense that the nodes keying material is periodically renewed by a set of leader nodes in order to enhance the system security. Although generic, our protocol is best suited to emergency ad hoc networks where the assumptions about the pre-configuration of the nodes with trusted keying material, and the existence of reliable leader nodes in charge of the renewal process are valid. By emergency ad hoc networks, we refer to the ad hoc networks consisting of the mobile nodes of the emergency workers like firemen or policemen that operate in the disaster area where no other communication infrastructure is existent or available. In this context, it is valid to assume that there are some leader nodes that can undertake in a reliable and trustworthy manner the task of the node public keys' renewal and that the communication devices used by the emergency workers are preconfigured with a keying material in a secure way before the deployment of the ad hoc network. Simulation results show that the performance of the protocol depends directly on the network connectivity, the number of leader nodes and the node mobility level.

The rest of the paper is organized as follows. Section 2 discusses the related work. Section 3 presents the proposed protocol, while Section 4 deals with the simulation setting and results.

2. PREVIOUS WORK

Several schemes have been developed to address the issue of trust establishment in ad hoc networks. A survey summarizing much of the related work on the field can be found in [15]. Some of these schemes are characterized by the existence of a central authority, whereas others follow a self-organized approach. Many trust establishment protocols rely on the notion of threshold cryptography, where instead of a single node acting like a certificate authority, several nodes in the network share this role. In this context, either some [18] or all [8] network nodes take part in issuing and verifying certificates. This is done to strengthen the protocol's resilience against attacks. Extending this idea, [11] introduces a mechanism that updates the keying material in the nodes forming the distributed certificate authority, resulting in improved robustness. In identity-based protocols [7] the node's identity is used as the node's public key, and a private key is provided by a set of nodes possessing shares of the network-wide private key. Various methods have been proposed [17][9] to produce identity-based public/private key pairs. Authors of [14] use two different types of public/private key pairs and crypto-based identifiers to enhance the protocol's robustness towards adversaries. In the certificate-chaining approach, indirect trust between nodes is established through the use of certificate exchange between intermediate nodes. Acceptable certificate chains are found using merged certificate repositories [3]. There are techniques that maximize the probability of finding a trust chain between any two nodes [12]. The effectiveness of such schemes can be proved through graph theory [13]. Pre-deployment strategies have also been proposed but their effectiveness is limited to the wireless sensor networks [5].

A lot of work in the field has been done in mobility-based schemes that take advantage of nodes' mobility to facilitate the key exchange and trust establishment [4]. In these cases, two nodes establish security association between each other by means of secure side channel communication or physical contact. Furthermore, solutions based on advanced cryptographic mechanisms like Diffie-Hellman have been proposed [2], that however are not applicable to emergency scenarios where there is need for fast and lightweight schemes. Hybrid schemes as the one in [16] try to combine advantages and to alleviate disadvantages of several approaches.

3. THE PROTOCOL

The proposed trust establishment protocol enables the nodes of an ad hoc network to establish security associations among each other in a distributed and peer-to-peer manner. The basis of the protocol is a node-to-node security handshake using a network-wide key that every node is preconfigured with. The protocol is dynamic in the sense that the nodes' keying material is periodically renewed by a set of leader nodes in order to enhance the system security. In defining the protocol, no assumption has been made regarding the routing protocol in use or the nodes' communication capabilities (e.g. secure side-channel).

In the initial stage, all the nodes are preconfigured with a private and public key pair and a network-wide key. When two nodes establish a security association between them, they also exchange information about which nodes each of them already trusts. The merged information is then forwarded by both nodes to their direct trusted neighbors in a

secure way. Thus, a secure network overlay is constructed in a distributed manner, where all nodes are securely associated with each other.

The established trust relationships are timely bounded. Therefore, a refresh mechanism is periodically performed in order to issue new certificates and securely transmit them to the nodes, before those currently in use expire. A set of *leader* nodes is responsible for the renewal process. The leader nodes are assumed to be reliable and resilient to security threats.

In Table 1 a comparison with representative works can be seen. The proposed protocol falls in the category of authority-based protocols that use preconfigured keying material that is periodically renewed. However, in contrast to other works does not use threshold or advanced cryptography mechanisms (e.g. Diffie-Hellman), while no special communication capabilities like a secure side-channel are either needed. This makes the protocol we present in this paper ideal for environments, where a fast and lightweight operation is required. Such scenarios are cases of emergency like forest fires, earthquakes and floods, where the network nodes are the firemen, policemen and medical staff. Interestingly, the above examples are, by definition, among the primary applications of the ad hoc networks. Furthermore, the assumptions made in the operation of the proposed protocol about the preconfiguration of the nodes with trusted keying material, and the existence of reliable leader nodes in charge of the renewal process suit perfectly in the setting of the emergency ad hoc networks. In these scenarios the networks consist of hierarchical groups of nodes that after leaving a common secure starting point, operate in the site of emergency. Therefore, the protocol presented in this paper mainly targets emergency ad hoc networks.

In what follows, we present in detail the two main functional blocks of the protocol: the trust establishment handshake between two nodes, and the renewal process of the nodes' keying material.

3.1 The trust establishment

When a node does not have valid security associations with other nodes, it executes a simple hello protocol, with a period of T_H seconds, in order to discover nodes located within its transmission range. If neighbors are detected, the trust establishment handshake is performed. When the security association is established, it is tagged with an expiration time, after which it is considered invalid. The lifetime T_L of each trust relationship is fixed for every node in the network. Every node maintains a list of nodes that it trusts and the corresponding time limits assigned to each trust relationship.

During the neighbor discovery mechanism, a node broadcasts a HELLO message and awaits for an acknowledgement (ACK-HELLO) indicating the existence of a node in its vicinity. None of these messages are encrypted, as they do not contain any sensitive information. Every node can reply to a HELLO message, even an adversary, but then it will have to prove its security credentials during the core trust establishment stage that begins upon the reception of the first ACK-HELLO packet. Any ACK-HELLO packets that may arrive later are discarded.

Having discovered a neighbor, the actual trust establishment handshake between the two nodes is performed. The node u initiating the whole trust establishment process sends

	Proposed protocol	[18]	[8]	[7]	[14]	[4]	[4]	[2]
Authority-based	✓	✓	✓	✓	-	-	✓	-
Preconfigured keys	✓	✓	✓	✓	-	-	✓	-
Key update mechanism	✓	✓	✓	-	✓	-	-	-
Threshold cryptography	-	✓	✓	✓	-	-	-	-
Advanced cryptography	-	-	-	-	✓	-	-	✓
Secure side-channel	-	-	-	-	-	✓	-	-

Table 1: Qualitative comparison between the proposed protocol and various trust establishment protocols

a JOIN packet containing its public key to the node v encrypted with the network-wide authority key that is preconfigured with. Node v decrypts the message with the same authority key and replies with a corresponding message encrypted by the same authority key. We will refer to this reply message as an ACCEPT message. In the ACCEPT message, node v includes apart from its own public key the information about the trust relationships with other nodes along with their time limits and public keys. Thus node u by establishing security association with node v , becomes member of the general secure overlay network where every node is trusted with all the others. The ACCEPT packet is then broadcasted to all nodes in the secure overlay network in a secure way since each transmission is made between trust related nodes. At each transmission between trusted nodes public key cryptography is used. The network-wide authority key is only used in the core trust establishment phase.

In order to avoid using any information from the routing layer, a controlled flooding mechanism is performed ensuring, by means of sequence numbers, that each node forwards each ACCEPT packet only once. As a result, all nodes of the secure overlay eventually share the same information regarding which nodes and until when, can be trusted.

3.2 The public key renewal

The network nodes are organised in a hierarchical manner. Apart from the normal nodes it is assumed that there is a set of leader nodes responsible for the nodes' keying material. Each leader node periodically, every T_K seconds, checks its local information about the time limits of the established trust relationships and issues new keys for the nodes whose trust time limit expires in time less than a critical margin T_C . The new certificate in the form of a REFRESH packet is propagated through the secure overlay network towards the interested node in a controlled flooding fashion, identical to the one followed in the case of the ACCEPT packets. Again each REFRESH packet is only forwarded once from each node to its direct trusted neighbors by using sequence numbers. This is done to avoid relying on any information from the routing layer.

When a node receives a newer version of its public key, it starts over trying to establish a new trust relationship with the first node discovered within its transmission range. The information regarding its new trust relationship is then propagated to all the nodes in the secure overlay network, including the leader nodes. If the certificate of a node expires before it receives a newer version, the node gets disconnected from the secure overlay without having the opportunity to reconnect.

4. SIMULATION

4.1 Setting

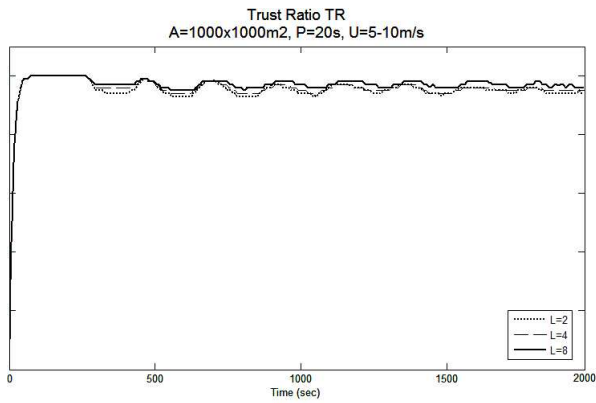
We implemented the proposed protocol in the Network Simulator ns-2 [10] in order to evaluate its performance in varying levels of network connectivity. The network studied in the simulations consists of 25 nodes, with fixed transmission range for all at 250 meters, moving in a square area whose edge equals to 500, 1000 or 1500 meters, according to the Random Waypoint Model [6]. This model dictates that each node randomly selects, following a uniform distribution, a point in the plane and moves towards it with a speed ranging uniformly between a minimum and a maximum value. In our experiments the speed intervals taken into account are 5-10 and 10-20 meters/sec. When it arrives there, it stops for a fixed period of time, equal to 20 seconds in our study, and then follows the same process. As MAC protocol, the 802.11b protocol is used.

As far as the protocol parameters are concerned, the security association lifetime T_L is taken to be 250 seconds, the critical margin T_C 50 seconds, the hello interval T_H 1 second and the local information check interval T_K 5 seconds. Finally, the number L of leader nodes is 2, 4 or 8 that are selected randomly following a uniform distribution. Each experiment is run 10 times and the values represented in the graphs are mean values of each set.

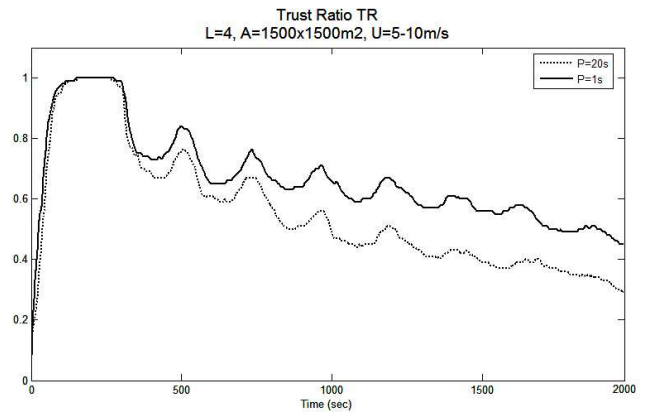
4.2 Results

The experiments are conducted in order to examine how the number L of leader nodes and varying levels of network density and node mobility affect the protocol's performance. The network density is taken into account through the network area size in which the nodes move, while the node mobility through the node pause time and speed. The basic metrics of interest in the simulation study of the protocol is the trust ratio TR and the convergence time C . The trust ratio TR at any instance is defined as the ratio of the number of the current established trust relationships over the maximum number of established trust relationships $N * (N - 1)$, where N is the number of the network nodes. Clearly, TR takes values ranging in $(0, 1]$. The convergence time C is taken to be the time required for all the security associations to be established, or in other words for the trust ratio TR to reach 1 for the first time. The convergence time C is independent of the number of leader nodes L .

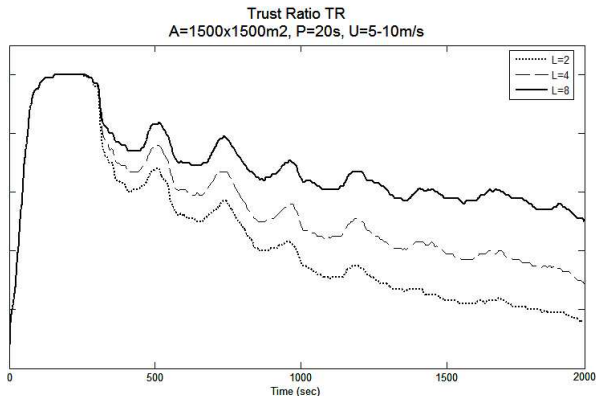
In Figure 1 the trust ratio TR of the protocol is depicted as a function of time for various cases of node movement area. When the area in which the node move is of $A = 1000 \times 1000 m^2$, the performance of the protocol falls since the network partitions are more frequent and thus some nodes are prevented from having their keying mate-



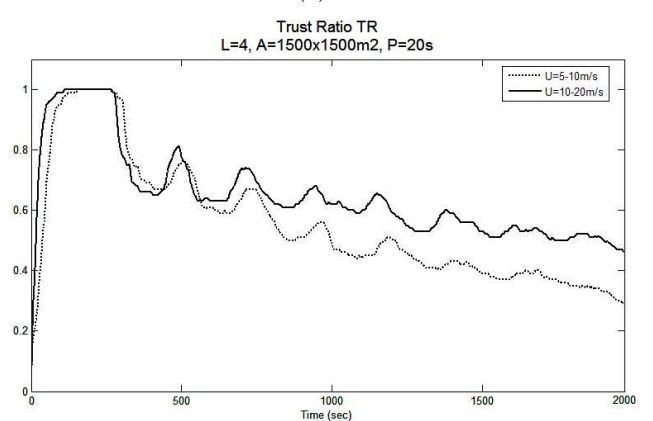
(a)



(a)



(b)



(b)

Figure 1: Illustrates the trust ratio TR of the protocol as a function of time for node pause time length $P = 20$ seconds, node speed $U = 5 - 10$ metres/second in the cases of mobile network in an area of (a) $A = 1000 \times 1000 m^2$, (b) $A = 1500 \times 1500 m^2$.

rial renewed. The protocol achieves values of TR smaller but close to 1 for all values of L . Even in the case of $L = 8$ the protocol maintains secure coverage of the network nodes of about 90%. In the case of network area $A = 1500 \times 1500 m^2$ the achieved trust ratio falls sharply for all values of L . The node density becomes so low, that the chances for trust establishment handshakes and successful dissemination of the ACCEPT and REFRESH packets in the network, decrease significantly. Even for the case of $L = 8$ the achieved TR is only around 60% at the end of the experiment. For smaller network areas the achieved TR was near 100% throughout the whole duration of the experiment.

In Figure 2 the trust ratio TR of the protocol is presented for number of leader nodes $L = 4$ as a function of the node mobility level, as this is described by the node pause time and maximum speed. The trust ratio TR grows with the node mobility since mobility helps to alleviate the low connectivity of the network on which both the trust establishment and the renewal process are dependent. When the nodes move more often, the information about established trust relationships and key refreshing is more likely to be successfully propagated across the network.

In Figure 3 the results regarding the convergence time

Figure 2: Illustrates the trust ratio TR of the protocol in the case of mobile network in an area of $A = 1500 \times 1500 m^2$ as a function of time for (a) varying node pause time length, and (b) varying node speed.

C as a function of the node mobility rate and the network area size are depicted. A general observation is that as the achieved convergence time C of the protocol grows as the node density or the node mobility rate decrease. Lower node density means that fewer connections are available between nodes and therefore, it becomes more difficult for trust establishments and their subsequent information propagation across the network to be completed successfully. However, in the cases of smaller network deployment area, the difference is not that significant. On the other hand, when the node movement area is larger, the protocol's convergence time C increases notably. This is explained by the fact that the smaller the area, the more frequent the packet retransmissions. Furthermore, the convergence time C decreases as the node mobility grows. Both when nodes move more often and when they move faster, the achieved C is lower. This is because the increased node mobility compensates for the low network connectivity.

5. CONCLUSIONS

This paper proposes a trust establishment protocol that enables the nodes of an ad hoc network to establish security

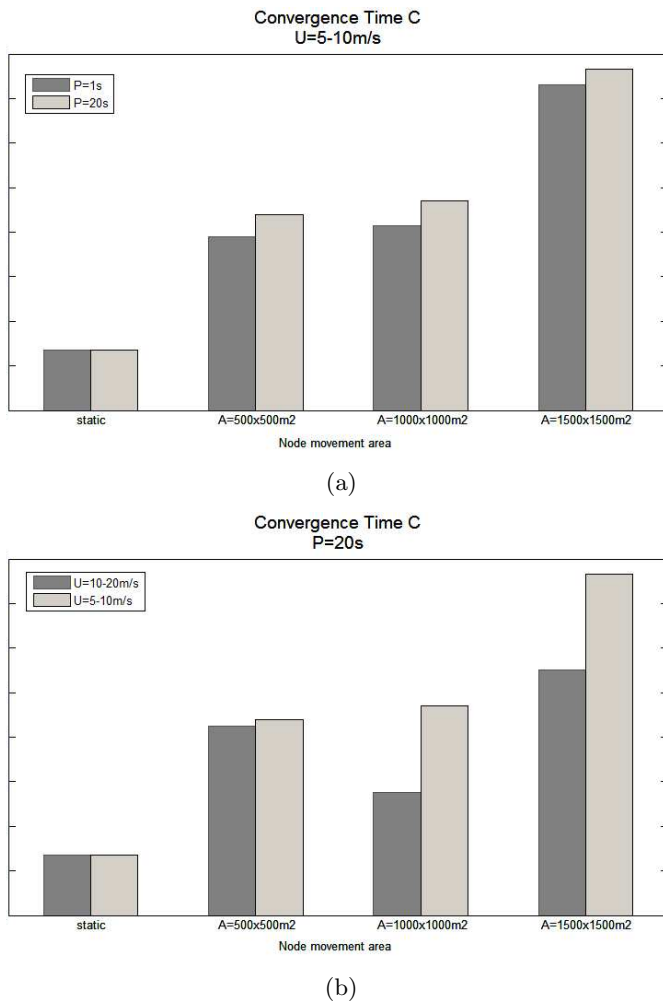


Figure 3: Illustrates the convergence time for various sizes of the node movement area with varying (a) node pause time length, and (b) node speed.

associations among each other in a distributed and peer-to-peer manner. The basis of the protocol is a node-to-node security handshake using a network-wide key that every node is preconfigured with. The protocol is dynamic in the sense that the nodes keying material is periodically renewed by a set of leader nodes in order to enhance the system security. Our protocol is best suited to emergency ad hoc networks. Simulation results show that the performance of the protocol depends directly on the network connectivity, the number of leader nodes and the node mobility level.

Acknowledgements

The authors wish to acknowledge the support of the ICT European Research Programme and all the partners in PEACE: PDMF&C, Instituto de Telecomunicaciones, FhG Fokus, Thales, Telefonica, Kingston University, Pale Blue.

6. REFERENCES

- [1] R.B. Bobba, L. Eschenauer, V.D. Gligor, W. Arbaugh, *Bootstrapping security associations for routing in mobile ad-hoc networks*, Proc. of the IEEE GLOBECOM, 2003.
- [2] M. Cagalj, S. Capkun, J.-P. Hubaux, *Key agreement in peer-to-peer wireless networks*, IEEE Special Issues on Cryptography and Security, 2006.
- [3] S. Capkun, L. Buttyan, J.-P. Hubaux, *Self-organized public-key management for mobile ad hoc networks*, IEEE Trans. on Mobile Computing **2**, no. 1, 52–64, 2003.
- [4] S. Capkun, J.-P. Hubaux, L. Buttyan, *Mobility helps security in ad hoc networks*, Proc. of the Int'l Symp. on Mobile Ad Hoc Networking and Computing, pp. 46–56, 2003.
- [5] L. Eschenauer, V.D. Gligor, *A key-management scheme for distributed sensor networks*, Proc. of the 9th ACM Conf. on Computer and Communications security, pp. 41–47, 2002.
- [6] D.B. Johnson, D.A. Maltz, *Dynamic source routing in ad hoc wireless networks*, Mobile Computing, vol. 353, Kluwer Academic Publishers, 1996.
- [7] A. Khalili, J. Katz, W.A. Arbaugh, *Toward secure key distribution in truly ad-hoc networks*, Symp. on Applications and the Internet Workshops, pp. 342–346, 2003.
- [8] J. Kong, P. Zerfos, H. Luo, S. Lu, L. Zhang, *Providing robust and ubiquitous security support for mobile ad-hoc networks*, Int'l Conf. on Network Protocols, pp. 251–260, 2001.
- [9] R. Li, J. Li, P. Liu, H.-H. Chen, *On-demand public-key management for mobile ad hoc networks*, Wireless Communications and Mobile Computing **6**, no. 3, 295–306, 2006.
- [10] *The NS-2 Simulator*, <http://www.isi.edu/nsnam/ns/>.
- [11] W. Peng, Y. Wang, E.K. Park, K. Makki, *Dynamic key management for secure routing in manet*, Wireless Communications and Mobile Computing **7**, no. 10, 1233–1241, 2007.
- [12] K. Ren, T. Li, Z. Wan, F. Bao, R.H. Deng, K. Kim, *Highly reliable trust establishment scheme in ad hoc networks*, Computer Networks **45**, 687–699, 2004.
- [13] J. Sen, P. Roy Chowdhury, I. Sengupta, *A distributed trust establishment scheme for mobile ad hoc networks*, Proc. of the Int'l Conf. on Computing: Theory and Applications, pp. 51–58, 2007.
- [14] J. van der Merwe, D. Dawoud, S. McDonald, *Fully self-organized peer-to-peer key management for mobile ad hoc networks*, Proc. of the ACM Workshop on Wireless Security, pp. 21–30, 2005.
- [15] J. van der Merwe, D. Dawoud, S. McDonald, *A survey on peer-to-peer key management for mobile ad hoc networks*, ACM Computing Surveys **39**, no. 1, 2007.
- [16] G. Wang, Q. Wang, J. Cao, M. Guo, *An effective trust establishment scheme for authentication in mobile ad-hoc networks*, 7th IEEE Int'l Conf. on Computer and Information Technology, pp. 479–754, 2007.
- [17] Y. Zhang, W. Liu, Y. Fang, *Securing mobile ad hoc networks with certificateless public keys*, IEEE Trans. on Dependable and Secure Computing **3**, no. 4, 386–399, 2006.
- [18] Z. Zhou, Z.J. Haas, *Securing ad hoc networks*, IEEE Network **13** (1999), no. 6, 24–30.