Demonstrating the security vulnerabilities of the Identity-based Key Management scheme for MANETs

Eduardo da Silva, Murilo Soares Lima and Luiz Carlos P. Albini
NR2 – Department of Informatics
Federal University of Paraná
Curitiba, Brazil
Email: {eduardos,mwsl06,albini}@inf.ufpr.br

***Abstract*— The next generation of mobile communications will merge the well-known infrastructured wireless networks and the infrastructureless mobile ad hoc networks. However, their natural characteristics make them vulnerable to numerous severe attacks, making security a major issue in such networks. Cryptography mechanisms, both symmetric and asymmetric, provide strong techniques against most vulnerabilities. Among the asymmetric ones, the Identity-Based (ID-based) cryptographic mechanisms are proposed to simplify key management and to reduce the memory storage cost. In ID-based schemes, the node or user identity is used as its public key, while the private key is still provided by an external entity. Among all ID-based key management schemes found in the literature, the Identity-based key management (IKM) is the most suitable for the mobile ad hoc networks environment. However, IKM does not consider the presence of malicious nodes in the system. This paper analyses the IKM operations, evaluating its communication performance and its effectiveness in scenarios under false accusation attacks. Results show that IKM is not efficient in terms of communication costs neither resistant to false accusation attacks.**

Keywords*— *Key Management. Security. Attacks. MANETs.

I. Introduction

Mobile ad hoc networks (MANETs) are infrastructureless, self-organized and autonomous networks, composed by wireless devices such as mobile phones, hand-held smartphones, laptops, PDAs, and tablets PC. Due to their flexibility and dynamic characteristics, such networks have been applied on scenarios as homeland security, disaster rescue, battlefield communication, inter-vehicular services, multi-user games, and conference meetings [1]. Furthermore, the next generation of mobile communications will merge the well-known infrastructured wireless networks and the infrastructureless mobile ad hoc networks [2], bringing the concepts of MANETs into daily use telecommunications.

MANETs characteristics make them highly vulnerable to security threats. Dynamic behavior allows network partitioning and disconnections, while the dynamic topology requires that all security mechanisms must be distributed. Distribute requirements facilitate malicious nodes to perform attacks, such as false accusation or impersonation [3].

Cryptography is the main technique used to ensure data communication security, providing integrity, authenticity, non-repudiation, and confidentiality. Traditional cryptographic systems can be divided into symmetric and asymmetric ones. Symmetric systems require less processing than asymmetric ones, but they are not scalable and nodes must share secret keys, either by a secure pre-established channel or before network formation. Therefore, symmetric systems are not suitable for MANETs [1]. On the other hand, traditional asymmetric systems, also called public key systems, require a trusted entity to perform certificate and key authentication. However, establishing a trusted entity in MANETs is a challenge, due to their decentralized organization and lack of trust model [4].

Both symmetric and asymmetric cryptographic algorithms require the use of pair-wised keys. The secure administration of such keys, known as key management, must consider generation, storage, distribution, protection and revocation of the keys, and also ensures availability to authentic nodes [5]. In MANETs, key management must also deal with dynamic topology and be self-organized and decentralized [6].

Several key management schemes for MANETs can be found in the literature [4], among them, the identity-based (ID-based) ones. These schemes have a simple key management process and reduced memory storage cost compared to other schemes [7], making them an attractive approach for MANETs [8]. In ID-based schemes, the node or user identity, such as an email or IP address, is used to derive its public key, while the private key is generally provided by an external entity. ID-based key management has been gaining interest recently, and has been used by routing protocols, cooperation mechanisms, cryptographic systems, and others.

Even though several ID-based schemes can be found in the literature [8]–[12], only the Identity-based Key Management (IKM) [11] addresses key revocation and key update in fully distributed fashion and analyzes communication costs. However, it was not evaluated under misbehavior attacks, such as false accusations, or considering network partitioning. This article provides such an evaluation showing that it is vulnerable to the false accusation attack and that its functionality can be compromised by the network partition.

The rest of the paper is organized as follows: Section II introduces the ID-based key management schemes for MANETs; Section III describes the IKM; Section IV shows the evaluation of IKM; finally, Section V has the conclusion and future work.

II. Identity-Based Key Management for MANETs

Some ID-based key management schemes for MANETs can be found in the literature [8]–[12]. The one proposed in [9] combines ID-based and threshold techniques. All nodes that initialize the MANET form a distributed PKG set. The Private Key Generator (PKG) establishes system parameters and preloads nodes with their keying materials. The public key of the nodes are their identities, while their private keys must be computed by the nodes of the PKG. The scheme assumes that identities are recorded in hardware and cannot be altered. However, this scheme does not address key revocation or key update.

The key management scheme proposed in [10] has two components: key generation and identity-based authentication. The key generation component provides the master key of the network and the public/private key pair for each node. The identity-based authentication provides end-to-end authentication and confidentiality between nodes. Like [9], this scheme does not address key revocation or update.

A scheme that uses noninteractive pairwise symmetric keys applying ID-based key agreement can be found in [8]. It assumes that all nodes are properly set up before network formation with public parameters and their corresponding private key by an external PKG. However, this scheme does not address either key revocation or update.

The identity-based authentication and key exchange (IDAKE) scheme [12] consists of two techniques: a basic IDAKE and a self-organized IDAKE. The basic IDAKE consists of two phases: the initialization phase with access to an external PKG and the running phase without access to it. In the self-organized IDAKE, all tasks are performed by the nodes, without any external PKG. The external PKG is emulated by a threshold scheme. However, the this version does not specify how private keys are distributed. The IDAKE computational complexity depends on the implementation of the key revocation and renewal algorithms.

A survey about ID-based key management for MANETs, discussing their approaches, strengths, weaknesses, and comparing their main features can be found in [13]. It is important to point out that none of the schemes above were evaluated considering malicious attacks. Other solutions can also be found in the literature [14]–[18]. However, such solutions are specific for some services not addressing crucial requirements of key management.

III. The Identity-Based Key Management for MANETs

In Identity-Based Key Management for MANETs (IKM) [11], each node has an ID-based public/private key pair, which is valid for the entire network lifetime. IKM consists of three phases: key predistribution, revocation and update. **Key predistribution** is a one-time process occurring during *network initialization*, in which an external PKG establishes a set of system parameters and preloads every node with its appropriate keying materials.

After network initialization, the PKG functionalities are assumed by the network. To distribute its functionalities, the PKG: (*i*) randomly chooses a number, K_{P2}, as network master-secret; (*ii*) selects n nodes to form the Distributed PKG (D-PKG); (*iii*) performs a (t,n)-threshold secret sharing of K_{P2} [19]. Using the (t,n)-threshold secret sharing, it guarantees that the master secret K_{P2} can be reconstructed through a jointly operation of at least t nodes from D-PKG.

Upon joining the network, node n_x receives its public/private key pair from the PKG. Further, node n_x also has a *phase-specific* public/private key pair, which is received from the D-PKGs and altered in each key update phase. IKM is composed of non-overlapping *key update phases*, aiming to prevent cryptanalysis. All communications are performed using phase specific keys, while node keys are used only to obtain phase keys during key update phases.

The **key revocation** phase is based on accusations. If node n_x suspects that node n_y is compromised, it sends a signed accusation to a subset of the D-PKG, aiming to revoke the key from node n_y. The subset of the D-PKG is unique for each node and computed using a function $\mathscr{F}$ which is known by all nodes. In other words, to accuse node n_y, node n_x must use function $\mathscr{F}$ to compute a subset L of the D-PKG with β nodes, and send the accusation to such nodes.

When a D-PKG node, say n_z, receives an accusation against n_y from n_x, it verifies the signature of n_x, ensures that n_x itself is not revoked, and saves the accusation for the entire current update phase. If node n_z receives γ accusations against n_y, it sends a partial key revocation signed with its own master secret part to the revocation leader. IKM assumes that the node with the smallest ID in L acts as the revocation leader. After receiving t partial key revocation against n_y, the revocation leader revokes the keys from n_y. If $\beta < t$, the revocation leader sends the accumulated accusations against n_y to the other $(t-\beta)$ nodes from the D-PKGs. These nodes respond with their partial key revocation after verifying the accusations. Then, the revocation leader floods the key revocation through the network to alert all other nodes that n_y has been compromised.

Finally, to prevent cryptanalysis and to limit the damage from compromised keys, IKM implements a **key update** mechanism. A new update phase p_{i+1} starts either when phase p_i reaches a time threshold or when the number of revoked nodes during p_i reaches a limit. To perform a key update phase, any node n_z, from the D-PKG initiates the update. Node n_z selects other $(t-1)$ nodes from the D-PKG and sends them a request. Each selected node generates a partial common private phase key and sends it to node n_z. Node n_z also generates a partial common private phase key and, upon receiving all $(t-1)$ replies, it constructs a complete common private phase key. Then, n_z propagates such key to all non-revoked nodes, using the scheme in [20].

IV. Evaluation of IKM

This section contains an analytical evaluation of IKM considering the main characteristics and requirements of MANETs. It also contains simulation results addressing the effectiveness of IKM under scenarios with false accusation attacks.

A. Analytical evaluation

When a node n_x wants to join the network, it must contact an external PKG to receive its keying material. After such that, n_x is able to contact the D-PKGs and request its *phase-specific* keys. However, establishing and maintaining a trusted external PKG can be a hard task and an undesirable requirement for MANETs. The absence of an external PKG after network initialization can block new nodes joining system. This can be a great weakness of IKM.

In IKM, it is considered and evaluated $t = n/2$. However, it is widely known that in secret sharing schemes, parameter t must be greater than $n/2$ to ensure that the system will be resistant to failures and the most byzantine attacks [19]. Assuming $t = n/2$, IKM makes the system vulnerable to node misbehavior, or to a particular MANET characteristic: network partitioning. Fig. 1a depicts a scenario in which IKM is configured to use a (3,6)-secret sharing scheme. After network initialization, nodes move freely and network is split into two partition, each one with 3 D-PKGs nodes (Fig. 1b). In such a scenario, nodes from the two partitions will be able to contact a functional D-PKG and key update and revoke operations are valid in both.

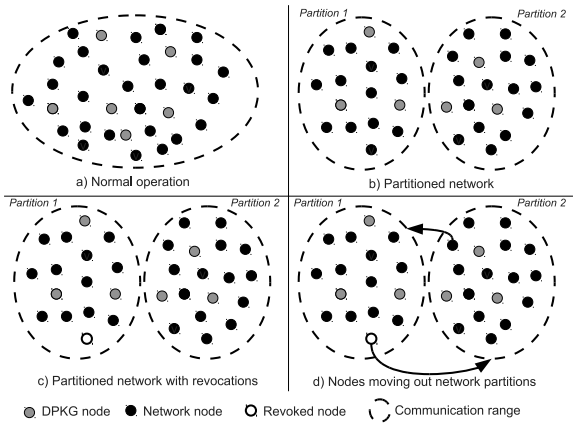

Fig. 1. Network partitioning in a (3,6)-secret sharing IKM scheme

Suppose the example illustrated in Fig. 1c. In this case, nodes in the first network partition can revoke the private key of a compromised node. As network is partitioned, nodes in the other partition will be not informed about the revocation, causing the D-PKG from both partitions to become uneven. In such a situation, the compromised node can move into the other partition and normally use its keys (Fig. 1d). Even if the compromised node has an out-of-date *phase-specific* key, it just waits until the next phase to receive a new version of its keys, as Fig. 2 illustrates.

Another issue is when unsynchronized key updates are performed in the partitions. Thus, one partition can be in phase p_i, while the other in phase p_j (Fig. 2d). In this case, if a node goes from one partition to the other it will not be able to use its keys. This problem is increased if the network is rejoined, as the network will have two distinct D-PKGs.

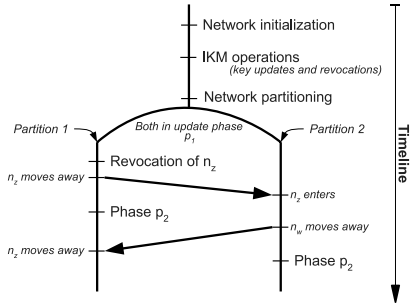

Fig. 2. Network partitioning in a (3,6)-secret sharing IKM scheme

One more weakness of IKM is that it has a number threshold parameters beyond n and t used in the secret sharing. IKM requires threshold parameters in several other operations. In key revocation, for example, β parameter represents the size of the set that will receive and handle accusations, and γ parameter is the quantity of required accusations against a node n_x in a time interval. Thus, any of these threshold parameters can be a point of attacks, and the system will be as secure as the weakest parameter defined.

B. Simulation Results

IKM was evaluated through simulations using Network Simulator 2.31, considering the same scenarios originally used in [11]. Simulations scenarios have 50 nodes in a square area of 700×700 m, with 250 m of transmission range. The medium access control protocol is the IEEE 802.11 DCF (Distributed Coordination Function), and the propagation model is two-ray ground. All scenarios were simulated using 5, 10 and $15m/s$ as the maximum speed of the units, though only results with $10m/s$ are reported below, as all other results are very similar. Table I shows all simulation parameters. The presented results are averages of 35 simulations with 95% of confidence interval.

TABLE I
SIMULATION PARAMETERS

Parameter	Used value
Network dimension	700 x 700
Transmission range	250 meters
Nodes	50 nodes
Mobility model	random waypoint
Propagation model	two-ray ground
Max. speed	5, 10 and 15 m/s
Max. pause time	5 seconds
(n,t)-secret sharing	(10,5) and (20,10)
β (Accusation holders)	1 to 10 nodes
γ (Required accusations)	equal to t
Attackers in collusion	γ to $\gamma+5$ nodes

Initially, IKM was evaluated in scenarios without the presence of malicious nodes. A system manager may configure $\beta = t$ to increase the system security. Theoretically, when $\beta = t$, IKM presents the best secure behavior against false accusations [11]. In such simulations, the number of accusers range from t to $t+5$ nodes. In other words, for

$(n = 10, t = 5)$, the number of accusers range from 5 to 10 nodes, while for $(n = 20, t = 10)$, it goes from 10 to 15 nodes. Fig. 3 presents the percentage of non-performed key revocations in scenarios without attacks and β equal to t. Results show that for $(n = 20, t = 10)$ and $\beta = 10$, IKM is not able to revoke the keys from compromised nodes, i.e the percentage of non-performed key revocations is 100%. This result is independent from the numbers of accusers. On the other hand, for $(n = 10, t = 5)$ and $\beta = 5$, the key revocation is more effective. However, for 14 attackers, the percentage of non-performed key revocation is greater than 60%.

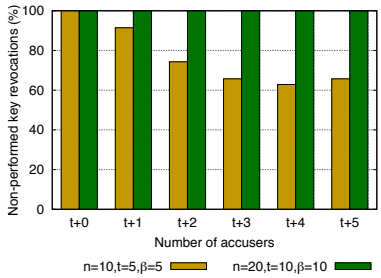

Fig. 3. Non-performed key revocation with $\beta = t$ and without attacks

Results from Fig. 3 shows that the system can be vulnerable to misbehavior node, due to the impossibility of revoking keys. On the other hand, if β is set with a small value, the system might be vulnerable to false accusations against honest nodes. Thus, IKM is also evaluated in scenarios with false accusation attacks with β ranging from 1 to 3 nodes. In such an attack, malicious nodes act in collusion to revoke keys of honest nodes, i.e. all malicious nodes issue a false accusation against a non-compromised node.

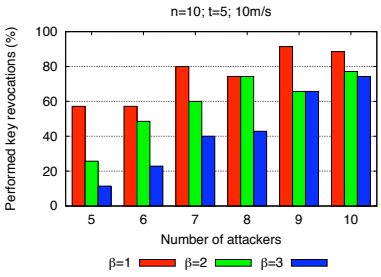

Fig. 4. Impact of false accusation when $n = 10, t = 5$

Fig. 4 and Fig. 5 show the impact of a false accusation attack against the IKM. In all simulations $\gamma = t$, i.e. when $t = 5$, it is necessary 5 accusations against node n_y from different nodes for the D-PKG to consider n_y as compromised. Fig. 4 depicts the impact of such an attack in scenarios with $(n = 10, t = 5)$ and β going from 1 to 3 nodes, the number of attackers (δ) goes from $\gamma(\delta = 5)$ to $\gamma + 5(\delta = 10)$ nodes. When $\beta = 1$ and $\delta = 5$, the percentage of successful attacks is almost 60%, reaching almost 95% when $\delta = 10$. Further, it is possible to notice that increasing β reduces the impact of such an attacks, although if $\beta = 3$ and $\delta = 9$ the percentage of compromised key revocations is greater than 60%.

Fig. 5 shows the impact of the false accusation attack in scenarios with $(n = 20, t = 10)$, β also ranging from 1 to 3 nodes, and δ going from $\gamma(\delta = 10)$ to $\gamma + 5(\delta = 15)$ nodes. In these scenarios, with $\beta = 1$ and $\delta = 10$, the percentage of successful attacks is almost 40%, reaching almost 98% when $\delta = 15$. Also, these results indicate that increasing the size of D-PKGS does not mitigates the vulnerability of IKM to such attacks, with $\beta = 3$ and $\delta = 15$, the percentage of compromised key revocations is almost 40%.

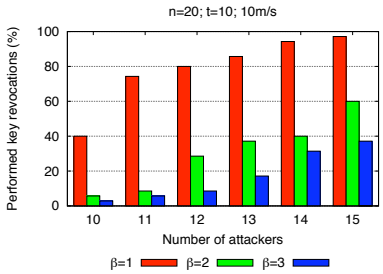

Fig. 5. Impact of false accusation when $n = 10, t = 5$

These results show that it is necessary to use large β values to increase the security of IKM against false accusation attacks. However, using a large β value might disable the entire revocation mechanism of IKM. Thus, the correct choice of β may have an impact on the behavior of IKM. A high value of β makes it less vulnerable to false accusation attacks, but it make difficult all correct revocations. On the other hand, a small value of β allows the correct functioning of the revocation mechanism, but makes the system vulnerable to such an attack. However, for any $\beta < t$, the system is vulnerable to the false accusation attacks disregarding the amount of malicious nodes.

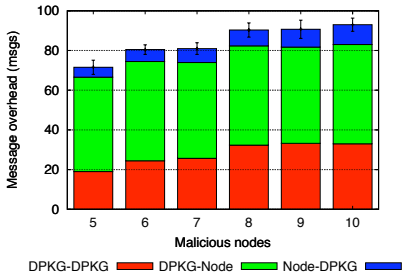

Fig. 6. Overhead of key revocation when $n = 10, t = 5, \beta = 1$

Finally, IKM was evaluated considering the communication overhead to perform the revocation of one key. Fig. 6 shows the communication overhead, in number of messages, when $(n = 10, t = 5)$ and $\beta = 1$. Note that, this is the scenario which presents the smallest overhead, as the revocation requires each accuser to contact one D-PKG node. Nevertheless, for 6 accuser nodes, IKM transmits close

to 80 messages to revoke a single key, approximately 60% are sent from the D-PKG to regular nodes and 30% are exchanged between D-PKG nodes.

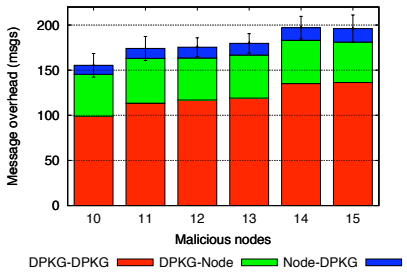

Fig. 7. Overhead of key revocation when $n = 20, t = 10, \beta = 1$

Fig. 7 shows the communication overhead, in number of messages, for $(n = 20, t = 10)$ and $\beta = 1$. As expected, such scenarios have a great overhead. If the number of accusers is 10, IKM transmits close to 150 messages to revoke a key. However, in these scenarios approximately 70% of the messages are exchanged between the D-PKG nodes.

V. Conclusion

The next generation of mobile communications will merge the well-known infrastructured wireless networks and the infrastructureless mobile ad hoc networks. However, MANETs characteristics make them highly vulnerable to security threats. Cryptography is the main technique employed to provide security in MANETs. Several key management schemes can be found in the literature, among them the identity-based (ID-based) key management is very attractive for MANETs. However, none of these schemes were evaluated considering malicious attacks.

Among all ID-based key management schemes, the Identity-based key management (IKM) is the most suitable for the mobile ad hoc networks environment. Thus, this work presents an evaluation of IKM effectiveness under the false accusation attack and submitted to a network partition.

Results show that the IKM scheme is vulnerable to false accusation attacks. In this scenarios, with $\beta = 1$ and the number of attackers equal to 15 nodes, the percentage of successful revocations through false accusations reaches almost 98%. On the other hand, with $\beta = 3$ and 15 attackers, the percentage of compromised key revocations is almost 40%. It also shows that to increase the security of IKM against false accusation attacks, it is necessary to use large β values. However, using a large β value might disable the entire revocation mechanism of IKM. For $\beta = t$, almost zero valid revocations are made in the system, while for any value $\beta < t$ the system is vulnerable to the false accusation attacks disregarding the amount of malicious nodes.

The overhead of IKM was also presented in number of messages to revoke a key. Future work includes the proposal of a secure ID-based key management, even in the presence of malicious nodes.

References

[1] I. Chlamtac, M. Conti, and J. J.-N. Liu, "Mobile ad hoc networking: imperatives and challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13–64, 2003.

[2] J. G. Jayanthi, S. A. Rabara, and A. R. M. Arokiaraj, "Ipv6 manet: An essential technology for future pervasive computing," *Communication Software and Networks, International Conference on*, vol. 0, pp. 466–470, 2010.

[3] B. Wu, J. Chen, J. Wu, and M. Cardei, *A survey on attacks and countermeasures in mobile ad hoc networks*. New York, NY, USA: Springer-Verlag, 2006, ch. 12, pp. 103–136.

[4] J. van der Merwe, D. Dawoud, and S. McDonald, "A survey on peer-to-peer key management for mobile ad hoc networks," *ACM Computing Survey*, vol. 39, no. 1, p. 1, 2007.

[5] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Danvers, MA, USA: CRC Press, 1996.

[6] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling, "A survey of key management in ad hoc networks," *IEEE Communications Surveys*, vol. 08, no. 03, pp. 48–66, 2006.

[7] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of Advances in Cryptology (CRYPTO 84)*. New York, NY, USA: Springer-Verlag New York, Inc., 1985, pp. 47–53.

[8] M. J. Bohio and A. Miri, "Efficient identity-based security schemes for ad hoc network routing protocols," *Ad Hoc Networks*, vol. 2, no. 3, pp. 309–317, 2004.

[9] A. Khalili, J. Katz, and W. A. Arbaugh, "Toward secure key distribution in truly ad-hoc networks," in *Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT '03)*. Washington, DC, USA: IEEE Computer Society, 2003, p. 342.

[10] H. Deng, A. Mukherjee, and D. P. Agrawal, "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)*, vol. 2. Washington, DC, USA: IEEE Computer Society, 2004, p. 107.

[11] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, no. 4, pp. 386–399, 2006.

[12] K. Hoeper and G. Gong, "Bootstrapping security in mobile ad hoc networks using identity-based schemes with key revocation," Centre for Applied Cryptographic Research, University of Waterloo, Waterloo, ON, Canada, Tech. Rep. CACR 2006-04, 2006.

[13] E. da Silva, M. N. Lima, A. L. dos Santos, and L. C. P. Albini, "Identity-based key management in mobile ad hoc networks: Techniques and applications," *IEEE Wireless Communications Magazine*, vol. 15, pp. 46–52, Oct 2008.

[14] Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon, "Ac-pki: anonymous and certificateless public-key infrastructure for mobile ad hoc networks," in *Proceedings of IEEE International Conference on Conference (ICC '05)*, vol. 5. IEEE Communications Society, 2005, pp. 3515–3519.

[15] L. Cai, J. Pan, X. S. Shen, and J. W. Mark, *Promoting Identity-Based Key Management in Wireless Ad Hoc Networks*, ser. Springer Series on Signals and Communication Technology. Springer-Verlag, 2007, pp. 88–102.

[16] N. Saxena, G. Tsudik, and J. H. Yi, "Identity-based access control for ad hoc groups," in *Proceedings of the International Conference on Information Security and Cryptology*, 2004.

[17] B.-N. Park and W. Lee, "Ismanet: A secure routing protocol using identity-based signcryption scheme for mobile ad-hoc networks," *IEICE Transactions on Communications*, vol. 88, no. 6, pp. 2548–2556, 2005.

[18] J. Pan, L. Cai, X. Shen, and J. W. Mark, "Identity-based secure collaboration in wireless ad hoc networks," *Computer Networks*, vol. 51, no. 3, pp. 853–865, 2007.

[19] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[20] D. Liu, P. Ning, and K. Sun, "Efficient self-healing group key distribution with revocation capability," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS '03)*. New York, NY, USA: ACM, 2003, pp. 231–240.