Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Efficient Authentication Scheme for Multicasting over Ad-hoc Networks

J.Jeyasoundari*, M.Monisha Devi, M.Saranya

IT&Bharath Niketan

Engineering College , India

Abstract— Ad-hoc networks are becoming an effective tool for many mission critical applications such as troop coordination in a combat field, situational awareness, etc. These applications are characterized by the hostile environment that they serve in and by the multicast-style of communication traffic. Therefore, authenticating the source and ensuring the integrity of the message traffic become a fundamental requirement for the operation and management of the network. However, the limited computation and communication resources, the large scale deployment and the unguaranteed connectivity to trusted authorities make known solutions for wired and single-hop wireless networks inappropriate. This work focus on providing Continuous Authentication for Multicast traffic for large scale dense ad-hoc networks. The continuous authentication combines the advantages of the time asymmetry and the secret information asymmetry paradigms in order to avoid message loss and provide data security. This work focus on network clustering scheme to reduce overhead due to computation and ensure scalability. Multicast traffic in a cluster employs message authentication codes (MACs) that are based on a set of keys in order to authenticate the message source. Message authentication codes (MACs) are based on a set of keys. Each cluster uses a unique subset of keys to look for its distinct combination of valid MACs in the message in order to authenticate the source. The confidentiality of source is provided by using RSA and DES algorithm during cross-cluster message transfer.

Keywords— Multicast communications, Message authentication, Confidentiality, Ad-hoc networks, Clustering.

I. INTRODUCTION

The continual advancement in wireless technologies has enabled networked-solutions for many nonconventional civil and military applications. In recent years ad-hoc networks have been attracting increased attention from the research and engineering community, motivated by applications like digital battlefield, asset tracking, air-borne safety, situational awareness, and border protection. In these network applications, it is important to devise efficient network management solutions suitable for nodes that are constrained in onboard energy and in their computation and communication capacities. In addition, the solutions must be scalable to support networks covering vast areas with a large set of nodes that communicate over many hops. These characteristics make the design and management of ad-hoc networks significantly challenging in comparison to contemporary networks. In addition, the great flexibility of ad-hoc networking comes at the price of an increased vulnerability to security attacks and trade-off would be unavoidable at the level of network management and services.

Multiple factors make multicast authentication in ad-hoc networks very challenging. The issues are fundamentally due to the resource constraints and the wireless links Group communication is considered a critical service in ad-hoc networks due to their inherently collaborative operations, where the nodes cooperate in network management and strive to accomplish common missions autonomously in highly unpredictable environment without reliance on infrastructure equipment. For example, in combat missions troops report their status and share observed data in order to become aware of the overall situation and coordinate their actions. In addition, it is common for ad-hoc networks to rely on multicast for management-related control traffic such as neighbour/route discovery to setup multi-hop paths, the establishment of time synchronization, etc. Such multicast traffic among the nodes has to be delivered in a secure and trusted manner. In particular the provided network services need to achieve the following security goals: Confidentiality, to prevent adversaries from reading transmitted data, Message integrity, to prevent tampering with transmitted messages, and Source Authentication, to prevent man-in-the-middle attacks that may replay transmitted data for node impersonation. Confidentiality is achieved by encrypting the transmitted data. The work presented in this paper aims at addressing the second and third goals. Providing an efficient multicast message and source authentication security service that can easily scale for large networks is an important capability for the operation and management of the underlying network. Source and message authentication is the corroboration that a message has not been changed and the sender of a message is as claimed to be. This can be done by sending a Cryptographic digital signature, or Message Authentication Code (MAC) .The first involves asymmetric cryptography and often needs heavy computation both at the sender and the receiver. The latter involves creating a message and source specific MAC that can be verified by the receiver. Thus, the MAC implicitly ensures message and source integrity.

This work focus on providing continuous Authentication for Multicast traffic for ad-hoc networks. This exploits network clustering in order to cut overhead and ensure scalability in ad-hoc networks. This projects focus on providing data security and data integrity to the message being multicasted. The network clusters will have nodes that lie within the cluster bandwidth. Each cluster will have a cluster head (CH), which enables secure data transfer within or cross cluster.

Here, the clustering strategy has two data transfer pattern as intra cluster and inter cluster/cross-cluster. Multicast traffic within the intra cluster or inter cluster employs Message authentication code (MAC) to authenticate the message source. Confidentiality of source is provided by RSA and double DES algorithm for encrypting the source. Intra cluster uses RSA algorithm to encrypt and decrypt source whereas inter cluster uses Double DES algorithm. To ensure that ad-hoc networks with clustering strategy cuts delay and ensure scalability.

II. RELATED WORK

R. Canetti *et al.*, R. Safavi-Naini and H. Wang worked on the asymmetry property denotes that a receiver can verify the message origin using the MAC in a packet without knowing how to generate the MAC. This property is the key for preventing impersonation of data sources. In secret information asymmetry every node is assigned a share in a secret, e.g., a set of keys. A source appends MACs for the multicast keys so that a receiver verifies the authenticity of the message without being able to forge the MACs for the other nodes. The challenge in using this category of approaches is striking the balance between collusion resilience and performance impact. While the use of a distinct MAC per node imposes prohibitive bandwidth overhead, relying on the uniqueness of the key combinations risks susceptibility to node collusion. A. Perrig, R. Canetti, D. Song, and D. Tygar employed on time asymmetry is to tie the validity of the MAC to a specific duration so that a forged packet can be discarded. One-way hash chains are usually employed to generate a series of keys so that a receiver can verify the current key based on an old key without being able to guess the future key. Initially, a source picks a key K0 and generates a chain of keys by recursively applying a one-way hashing function. These keys are used to form the MAC for the individual data packets. The source then reveals the last key, *Kl*, in the chain to all receivers to serve as the baseline for verification. The key which is used to generate the MAC of a packet is revealed after some time period so that the key cannot be used to impersonate the source. When revealed, the receiver validates the key using *Kl* or any of the previously revealed keys. Timed Efficient Stream Loss-tolerant Authentication (TESLA) is a very popular example of this category. One of the most distinct advantages of time asymmetry is the minimal per packet overhead that they impose. A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P. Spilling employed on the idea to use an upper tier as a trusted authority for key generation. Published approaches vary in selecting the private key generator among the nodes in the higher tier and on the level of coordination among these nodes. R. Gennaro, *et al* used ID-based threshold system in order to provision resilience to a node compromise in the upper tier, while others use key subsets that are distributed among multiple nodes. M.Younis, O. Farrag, and S. Lee worked that each cluster is controlled by a cluster-head, which is reachable to all nodes in its cluster, either directly or over multi-hop paths. Nodes that have links to peers in other clusters would serve as gateways. The presence of gateways between two clusters implies that the heads of these clusters are reachable to each other over multi-hop path and that these two clusters are considered neighbors. If a node moves out its current cluster and joins another, it is assumed that the associated cluster-heads will conduct a handoff to update each other about the change in membership of their clusters; other cluster-heads will not be involved in the handoff events outside their clusters.

III. PROPOSED METHODOLOGY

A. Problem Statement

An ad-hoc network is a collection of autonomous nodes that together set up a topology without the support of a physical networking infrastructure. Communications among nodes are via multihop routes using all directional wireless broadcasts with limited transmission range. The aim is to eliminate any need for interaction with the authority to retrieve the public key of some nodes in the network with a known one-way hash cryptographic function. This paper mainly considers an adversary who tries to manipulate the system through capturing and compromising some nodes. When a node is captured, its memory can be read or tampered with. Therefore, an adversary would know the keys of a compromised node. In addition, the operation of a compromised node may be manipulated to launch attacks such as replay, impersonation, etc. Here it focus to ensure source and message authentication in order to counter modify, replay and impersonation attacks. In the system model considered in this paper, nodes are grouped into clusters. The clusters formation can be based on location and radio connectivity.

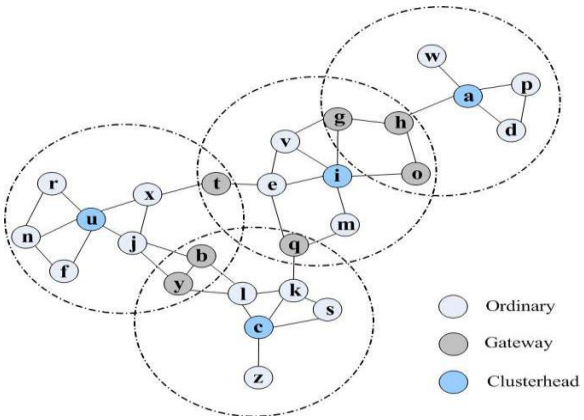

Fig. 1 A clustered Ad-hoc Network where each node reaches its cluster head

B. Cluster formation

Clustering is a popular architectural mechanism for enabling scalability of network management functions. It has been shown that clustered network topologies better support routing of multicast traffic and the performance gain dominates the overhead of creating and maintaining the clusters. All nodes in network have some computing power and processing power while transmitting data. Each node in the network is assigned a unique ID. Then each node broadcasts a HELLO message to have knowledge of its neighbour nodes, which can be used to calculate its degree d. Here clustering is done by assigning bandwidth range so that nodes under particular bandwidth are clustered accordingly.
S_r (i) denotes the size of cluster i. A non cluster node should take account of this factor to decide which cluster to join in r^{th} round. The formula used to depict the criteria that considers both the residual energy of cluster head and the size of the cluster is listed as follows

$$Vj(\ i,r\ ) = \lambda E_i^r + (1-\lambda)\ \left(\frac{N}{K} - S^r(i)\right) \quad \text{---- (1)}$$

Where λ is a factor used to adjust the impact of *Sr* (*i*) and E_i^r which can be obtained by experiments. When a node is far away from all cluster heads, it can utilize formula 1 to choose its cluster head which has more residual energy and smaller cluster size than other cluster heads. This criterion will bring a better load balancing to cluster heads and increase the performance.

C. Cluster Head

Generally cluster selection is done either manually which is needs more energy consumption. This is relatively expensive when nodes transfer data in cluster. Here, Cluster head selection is done by using election algorithm based on unique ID and computing power .This enable to reduce energy consumption for data transfer from source to remote receivers. So the residual energy of node is the main criteria for the election of cluster head. Furthermore, data aggregation can save considerable energy when the source nodes forming one cluster are distributed in a relatively small region while the node is far away from the source nodes, because nodes only need much few. Due to the deduction above, an election weight taking account of the residual energy and the concentration degree of nodes are introduced in Election algorithm for cluster-head election.

Given a wireless networks of N nodes 1, 2… N, D^r (i) is defined to be the concentration degree of node i, namely the number of nodes it can sense during the r^{th} round.

W (j, r) is defined as the election weight of node *j* in r^{th} round,

$$\lambda = {}^{1}/_{1+\beta} \qquad \beta = \frac{E_i^r}{E_j}$$

$$w(i,j) = \alpha \frac{E_j^r}{E^r} + (1-\alpha)\frac{D^r(j)}{\frac{N-1}{K}} \qquad \text{--- (2)}$$

Where *K* is the number of clusters, E_j is the initial energy of node *j*; E^r is the average residual energy of network in r^{th} round. *β* denotes the residual energy of node *j* in round *r*. *α* is an adaptive factor to adjust the impact of residual energy and concentration degree to election weight. With the reduction of residual energy, *α* will gradually increases to adapt to the decrease of the number of effective nodes in ad-hoc networks.

D. Central Authority

Central authority (CA) is constructed to generate and distribute public and private to nodes in cluster. Each CH of its cluster will indicate CA about the addition of new node in cluster in order to generate its key. As in previous work, nodes will have their keys which are attacked by adversary to reveal the key. Here CA is constructed in order to prevent impersonate and replay attack. Thus CA prevents node compromise to within a cluster.

E. Message Authentication Code(MAC)

Message Authentication code (MAC) algorithm is used to provide authentication to the message. MAC generates a fixed length authenticator. The fixed length authenticator is a cryptographic checksum, which is generated by a function C.

MAC=C (K, M)

Where *M is* variable length message, *K* is secret key shared only by sender and receiver and *C(K,M)* is fixed length authenticator.MAC performed in two steps (i.e.) first step to generate MAC code to append with message and second, to regenerate MAC code to verify integrity.

Step 1: Given M1, compute MAC1
MAC1=C (K1, M1) for all 2^k keys
Number of matches=$2^{(k-n)}$
Step 2: Given M2, compute MAC2
MACi=C (K, M2) for all $2^{(k-n)}$ keys resulting from step 1.
Number of matches=$2^{(k-2xn)}$
Step 2 is done to regenerate MAC code in order to verify authentication of message.

IV. EXPERIMENTS AND RESULTS

A two-tier process for authenticating multicast traffic in ad-hoc networks. Continuous authentication is implied by clustering to partition a network, and then authenticates multicast traffic by employing time asymmetry and secret information asymmetry for intra-cluster traffic and inter-cluster traffic. As mentioned earlier, clustering is a popular scheme for supporting scalable network operation and management. Several studies have shown that the gains achieved by clustering supersede the overheard in forming and maintain the clusters. It leverages such a network management scheme. In this work data transfer is based on either intra or inter cluster. The user can select the sender node and receiver node to transmit the data. From the selection of the receiver the intra cluster or inter cluster is determined.

A. Intra Cluster Data Transfer

Here, Intra cluster uses RSA algorithm to encrypt and decrypt the source message. Consider cluster *a* has Nodes *a1, a2…a_n.* Node *a1* multicast source message to all other nodes in cluster *a (i.e.) to a2, a3…a_n.* Intra cluster follows 3 steps as,

Step 1: MAC authentication is performed to source message and then it is encrypted by RSA to provide data security.
Step 2: The encrypted message is sent to its cluster head.
Step 3: The encrypted message is sent to the multicast receivers to decrypt the message. After decrypting, message is verified by regenerating MAC code to verify data integrity.

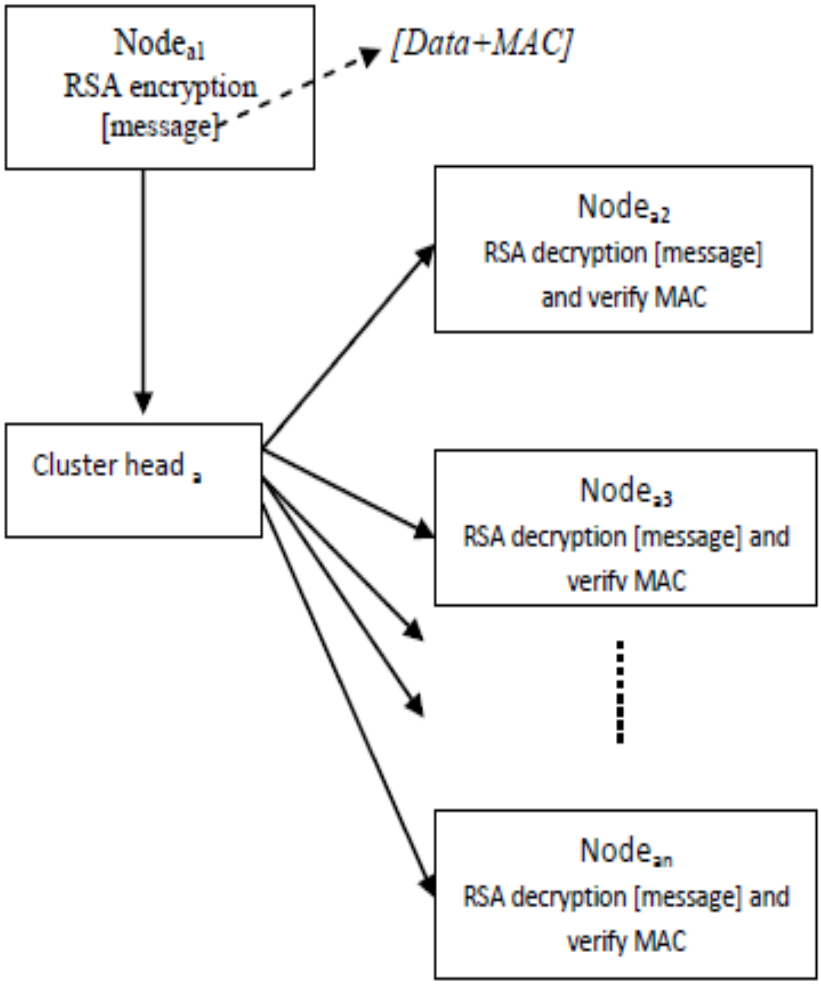

Fig. 2 Intra cluster data transfer

B. Inter Cluster Data Transfer

Here, Inter cluster uses double DES algorithm to encrypt and decrypt the source message to provide data security to message transferred. Consider cluster *i, j, g and h.* Node *'s'* that belongs to cluster *i* sends multicast message to receivers in cluster *j , g and h*. It involves following steps in inter cluster multicasting as,

Step 1: MAC authentication is performed to source message at *s* and then it is encrypted by DES algorithm to provide data security.
Step 2: The encrypted message is sent to its cluster head CH_i. Once again the data encrypted by DES algorithm at CH_i.
Step 3: The double encrypted message is sent by CH_i to CHj, CH_g and CH_h of multicast receivers to decrypt the message.
Step 4: Decrypted message from CH_j, CH_g and CH_h is sent to its respective receiver nodes as node j1, g2, h1., where message is decrypted once again due to double DES encryption. After decrypting, message is verified by regenerating MAC code to verify data integrity.

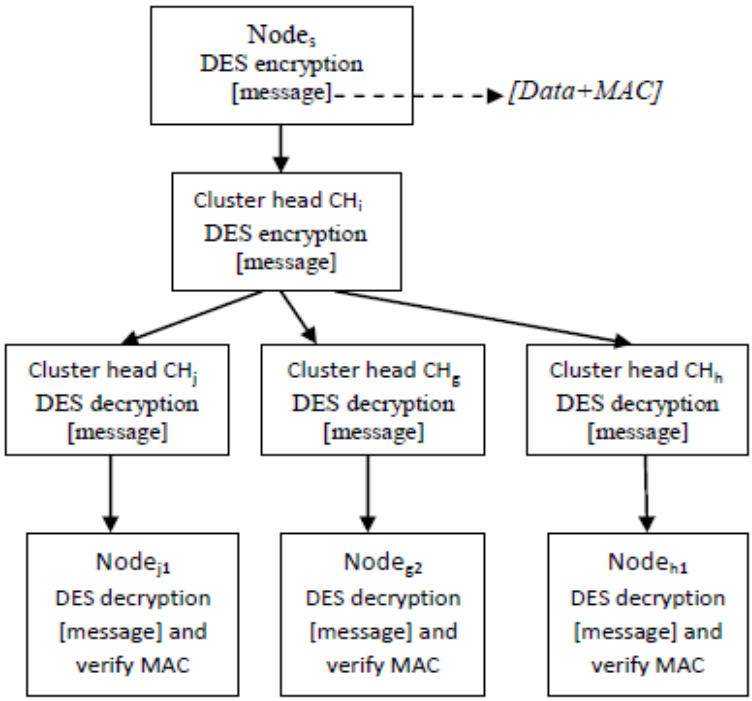

Fig. 3 Inter Cluster data transfer

C. Cluster Head Selection

Cluster head is nominated based on node ID and computation energy. So number of nodes and cluster is needed to be calculated. This is done by assuming d is the maximum degree a node in network. The ideal multicast tree will then be a balanced tree of degree equals d rooted at the source node. Assuming that it is feasible to construct such a balanced multicast tree, the number of transmissions will depend on the height *h* of the tree. In general, there are *d* nodes in the first level, *d*2 nodes in the second level, etc. Thus,

Number of nodes in a balanced tree of degree d =

$$1+d+d^2+\ldots.+d^h = \frac{d^{h+1}}{d-1} - 1$$

T he average number of clusters Nch = $\lceil 1/p \rceil$

T he average number of a cluster Nc = $\lceil N \; x \; p \rceil$

The average number of nodes in a *k*-hop cluster can be estimated as follows. The probability *Pc* that a node is in a cluster equals the probability that it is at most *k* hops away of a cluster-head, i.e., less than a distance $k \times Tr$ away from the cluster-head.

$$P_c = \frac{(\pi k^2 T_r^2)}{L^2}$$

The average number of clusters in that case is:

$$N_{ch} = \left\lceil \frac{1}{P_c} \right\rceil = \left\lceil \frac{N}{k^2 d_{avg}} \right\rceil$$

D. Baseline Performance

Election algorithm for Cluster head Selection enables to reduce previous work, Bandwidth overhead increased due to signing every packet using asymmetric keys. It includes impersonation and replay attack .This is overcome by using CA to distribute public/ private key pairs, which is used to establish initial trust.

The Continuous authentications of multicasting involve distinct procedures for intra and inter-cluster operations. For the intra-cluster multicast, the cluster head forwards the packet over a tree and employs a time asymmetry based authentication protocol that requires only a single MAC per packet. For a multicast that extends outside the source's cluster, an inter cluster procedure is invoked to deliver the packet to the cluster heads of the participating receivers. Each cluster-head will then locally multicast the packet within its cluster. Thus, the number of transmissions is the sum of all local (intra-cluster) multicasts inside the individual clusters and the multicast from the source node to the other cluster-heads in the network.

E. Effect of MAC

Here it demonstrates the performance advantage of continuous authentication of multicasting in terms of the bandwidth overhead. When using a MAC combination, rather than a single MAC per node, continuous authentication of

multicasting introduces a minimal overhead that slightly grows as the number of nodes increases. However, using a single MAC per node boosts the overhead substantially. The bandwidth overhead under a single MAC per node is significantly more than the baseline with MAC combinations. This indicates the dominance of the effect of the MAC size on performance. Continuous authentication of multicasting scales very well, even when a single MAC per node is used.

V. CONCLUSION AND FUTURE WORK

In recent years there has been a growing interest in the use of ad-hoc networks in security-sensitive applications such as digital battlefield, situation awareness, and border protection .The collaborative nature of these applications makes multicast traffic very common. Securing such traffic is of great importance, particularly authenticating the source and message to prevent any infiltration attempts by an intruder. Contemporary source authentication schemes found in the literature either introduce excessive overhead or do not scale for large networks. This paper has presented Continuous authentication of multicasting, which pursues a two tired hierarchical strategy combining both time and secret-information asymmetry in order to achieve scalability and resource efficiency. The performance has been increased with Central authority and election algorithm for CH selection confirming its effectiveness. Continuous authentication of multicasting with clustering limits the effect of a node compromise to within a cluster. Clustering enables to perform 2 or 3 hops providing security and performance.

Future work includes the effect of different clustering strategies in Ad-hoc network with multicasting and increasing multiple hop communication.

REFERENCES

[1] Mohamed Younis"TAM: A Tiered Authentication of Multicast Protocol for Ad-Hoc Networks" IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 9, NO. 1, MARCH 2012.

[2] 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 Commun. Surveys & Tutorials*, vol. 8, no. 3, pp. 48–66, Dec. 2006.

[3] Yuzhong Chen, and Yiping Chen"An Energy Efficient Clustering Algorithm Based on Residual Energy and Concentration Degree in Wireless Sensor Networks "*Huangshan, P. R. China, 26-28,Dec. 2009, pp. 306-309*

[4] R. Safavi-Naini and H. Wang, "Multi-receiver authentication codes:models, bounds, constructions, and extensions," *Inf. Computation*, vol.151, no. 1–2, pp. 148–172, May 1999.

[5] Xiaoguang Niu, Zhihua Tao, Gongyi Wu, Changcheng Huang, Li Cui "Hybrid Cluster Routing: An Efficient Routing Protocol for Mobile Ad Hoc Networks" *IEEE ICC 2006 proceedings*

[6] Sudarshan Vasudevan, Jim Kurose, Don Towsley "Design and Analysis of a Leader Election Algorithm for Mobile Ad Hoc Networks" National Science Foundation under grants ANI-0085848 and EEC-0313747001.

[7] J. Y. Yu and P. H. J. Chong, "A survey of clustering schemes for mobile ad hoc networks," *IEEE Commun. Surveys & Tutorials*, vol. 1, no. 1, pp. 31–48, 2005.

[8] P. B. Velloso, *et al.*, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Trans. Network Service Management*, vol. 7, no. 3, Sep. 2010.

[9] Dewan Tanvir Ahmed "Multicasting in Ad Hoc Networks" Wireless Ad Hoc Networking Professor Ivan Stojmenovic Ottawa, Ontario, Canada, Fall 2005

[10] L. Junhai, Y. Danxia, X. Liu, and F. Mingyu, "A survey of multicast routing protocols for mobile ad-hoc networks," *IEEE Commun. Surveys & Tutorials*, vol. 11, no. 1, pp. 78–91, first quarter 2009.

[11] H. Yang, *et al.*, "Security in mobile ad-hoc wireless networks: challenges and solutions," *IEEE Wireless Commun. Mag.*, vol. 11, no. 1, pp. 1536– 1284, Feb. 2004.

[12] R. Canetti *et al.*, "Multicast security: a taxonomy and efficient constructions,"in *Proc. 1999 IEEE INFOCOM*.

[13] Perrig, *et al.*, "Efficient and secure source authentication for multicast," in *Proc. 2001 Network Distributed System Security Symposium*.

[14] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," in *Proc. 2001 ACM Conf. Computer Commun. Security*.

[15] E. C. H. Ngai and M. R. Lyu, "An authentication service based on trust and clustering in wireless ad hoc networks: description and security evaluation," in *Proc. 2006 IEEE International Conf. Sensor Networks, Ubiquitous, Trustworthy Computing*.

