Cross-Layer Design for Energy-Efficient Secure Multicast Communications in Ad Hoc Networks

Loukas Lazos and Radha Poovendran
{l_lazos, radha}@ee.washington.edu
Network Security Lab, Dept. of EE,
University of Washington, Seattle, WA

***Abstract*— We consider the problem of secure multicast in an energy-constrained wireless environment. We present an analytical formulation of the energy expenditure associated with the communication overhead of key management and highlight its dependence on the network topology and the key distribution method. We show that the optimal solution of this formulation does not scale with multicast group size and propose a sub-optimal, cross-layer, low-complexity algorithm for energy efficient key distribution. We present simulation studies that show the energy savings achieved by our scheme and compare its performance when different routing algorithms are employed.**

I. Introduction

Wireless ad hoc networks operate without a pre-deployed infrastructure. Due to their high degree of flexibility and self-configurability, they have become one of the most attractive solutions for rapidly interconnecting a large number of mobile personal devices. Most of the sensors are battery-operated and hence, constrained in communication and computational capabilities. The power consumption due to computation has been significantly reducing due to advances in silicon technologies[1]. However, the power consumption due to communication is significantly affected by the physical properties of the medium of signal propagation and is the most dominant factor in battery depletion [1].

Many group applications already implemented in wired networks will be extended to wireless ad hoc networks. Multicast is the most suitable model for reducing the incurring network load, when traffic needs to be securely delivered from a single authorized sender to a large group of valid receivers. Provision of security for multicast sessions is realized through encrypting the session traffic with cryptographic keys. All multicast members must hold valid keys in order to be able to decrypt the received information.

The problem of distributing and updating the cryptographic keys to valid members, known as key management, adds storage, communication and computational overhead to the network management. Key updates are required either periodically or on-demand, to accommodate membership changes, including additions and deletions, in multicast groups. Security being a network management problem, should consume as minimal energy as possible in updating the keys. In wireless ad hoc networks where nodes are dependent upon batteries, excessive overhead can lead to rapid battery depletion, resulting in lack of network connectivity and/or termination of essential network services. While satisfying typical constraints such as bandwidth, complexity and storage is a must for providing multicast services, node energy preservation is one of the most crucial parameters for ensuring network operation in an wireless ad hoc environment. Energy is a physical layer parameter, while security is an application layer service. Hence, the energy-efficient design has to take the cross-layer interaction into consideration.

In this paper, we study the problem of energy-efficient multicast key distribution. We first present an analytical formulation based on energy-expenditure due to re-keying and jointly consider the physical, network and application layers in the formulation. By making use of the minimum weight non-bipartite matching problem (MWNBM) [2], we show that for a multicast group with N members, a candidate optimal solution for minimizing the energy expenditure has at least $\mathcal{O}(N^3)$ complexity. We then present a sub-optimal, cross-layer algorithms that considers the node transmission power (physical layer property) and the multicast routing tree (network layer property) in order to construct an energy-efficient key distribution scheme (application layer property).

After showing that the cross-layer design has to make use of underlying broadcast routing, we analyze the impact of recently proposed multicast routing protocols on the energy expenditure due to key updated communication overhead. We consider power-efficient multicast routing algorithms such as the *Broadcast Incremental Power* (BIP) [3], the *Embedded Wireless Multicast Advantage* (EWMA) [4], the *Minimum Spanning Tree* (MST) [5] and the *Shortest Path Routing* (SPR) [5]. As an interesting observation, we show that the most energy-efficient broadcast routing may not be the most suitable one for energy-efficient key distribution. This is due to the fact that re-keying requires different keys to be transmitted to different sub-groups, while broadcast routing tries to reach as many nodes as possible at once.

The remainder of the paper is organized as follows. In Section II we present notation and background information. In Section III we describe the network model assumptions. In Section IV we formulate the routing-aware key distribution problem as an optimization problem and derive the complexity of the optimal solution. We then develop a sub-optimal energy-efficient routing-aware key distribution algorithm. In Section V, we provide simulation results to show the improvements achieved by our algorithms and compare the performance of our scheme under different routing algorithms. In Section VI we present conclusions.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2004		**00-00-2004 to 00-00-2004**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cross-Layer Design for Energy-Efficient Secure Multicast Communications in Ad Hoc Networks	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **University of Washington,Department of Electrical Engineering,Seattle,WA,98195**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

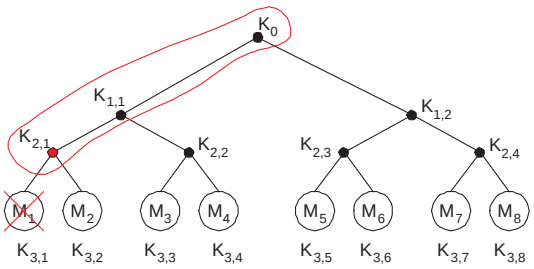
12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**7**	



(a)

$$
\begin{aligned}
GC \rightarrow M_2: &\quad \{K'_{2.1}\}_{K_{3.2}}, \{K'_{1.1}\}_{K_{3.2}} \\
GC \rightarrow \{M_3, M_4\}: &\quad \{K'_{1.1}\}_{K_{2.2}} \\
GC \rightarrow \{M_2 - M_4\}: &\quad \{K'_0\}_{K'_{1.1}} \\
GC \rightarrow \{M_5 - M_8\}: &\quad \{K'_0\}_{K_{1.2}}
\end{aligned}
$$

(b)

Fig. 1. (a) M_1 leaves the multicast group in a binary key tree, (b) Update messages sent by the GC to valid members.

II. Notation and Background

A. Notation

The following notations will be used through the rest of the paper.

N	Multicast group size.
T	Key distribution tree of height h. The root has level $l = 0$.
$K_{l.j}$	Key assigned to the j_{th} node of the l_{th} level of the tree T.
M_i	The i_{th} member of the multicast group.
GC	Group controller of the multicast group.
$G(V, A)$	An undirected graph with a set of vertices V and a set of edges A.
R	The routing tree of an ad hoc network.
$\{m\}_{K_{l.j}}$	Message m encrypted with key $K_{l.j}$.
$B \rightarrow S : m$	B sends a message m to all members of subset S.
$S_{l.j}(T)$	Set of members holding the key $K_{l.j}$

B. A review of group key management techniques

When secure communications involve large dynamic groups with frequent membership changes, the key management/distribution scheme needs to be scalable with the group size. The number of updated keys after a member leave is significantly higher than the updated keys after a member join [6], [7]. Hence, key management schemes mainly address the overhead of a member (or multiple members) leave.

Scalable solutions in both communication cost and storage requirements group key management techniques that have been proposed for group communication in wired networks make use of logical key trees [6], [7], [8], [9]. Logical key tree based schemes reduce the complexity of re-keying operation after a member leave from $\mathcal{O}(N)$ (Trees of degree N) to $\mathcal{O}(logN)$ [6]. The storage requirement of a member in a logical key tree is also $\mathcal{O}(logN)$.

In Figure 1(a), we present a key distribution tree for a multicast group of $N = 8$ members plus the GC. Each member is assigned keys that are along the path traced from the leaf node to the root [6]. For example M_1 is assigned keys $\{K_0, K_{1.1}, K_{2.1}, K_{3.1}\}$. If M_1 leaves the multicast group keys $\{K_0, K_{1.1}, K_{2.1}\}$ need to be updated by new keys denoted as $K'_{i.j}$ and the GC needs to send the update messages shown in Figure 1(b) to the remaining valid members.

C. Broadcast routing in ad hoc networks

The broadcast routing service provided by the network layer, is establishing the appropriate paths for reaching all nodes of the network, from a single sender. The routing algorithms are aiming at minimizing the total energy for broadcasting a message to every member of the multicast group. The network management problem of finding a broadcast tree with minimum total transmit power is known to be NP-hard [3], [4], [10]. Several heuristic algorithms have been recently developed for power-efficient broadcasting with sub-optimal performance [3], [4], [10]. Most of the heuristics attempt to fully exploit the *wireless broadcast advantage*.

To the best of our knowledge, the impact of broadcast routing algorithms on the efficiency of the key distribution has not been studied before. One might expect that a routing algorithm that minimizes the total transmit power will perform efficiently in the key distribution. However, rekeying of valid members involves transmissions to sub-groups of different size.

Lets consider the case of member M_1 leaving the multicast group in Figure 1(a). The keys to be updated are already marked. According to Figure 1(b), there are two unicast transmissions to $\{M_2\}$, one sub-group transmission to $\{M_3, M_4\}$, one sub-group transmission to $\{M_2, M_3, M_4\}$ and one to $\{M_5 - M_8\}$. Routing algorithms optimized for broadcast transmission need not be efficient for unicast or sub-group transmissions. We will investigate the impact of recently proposed power-efficient routing algorithms on the energy consumption due to key management.

It is also possible to formulate the problem to choose the routing that will optimize the key update communications. However, we note that the communication overhead for re-keying is relatively small compared to the session traffic. Hence, it would be unreasonable to optimize the routing tree for minimizing the energy expenditure due to the overhead. Instead, we will examine what is the performance of our key distribution scheme when various routing algorithms are employed.

III. Network Model

We assume that the network consists of N members of a multicast group plus the GC, randomly distributed in a

specific area. We consider a single-sender multiple-receiver communication model. We also assume that any node can act as relay node and the communication range is constrained by the node's maximum transmission power. The nodes of the network are assumed to be static (no mobility is incorporated).

The network nodes are assumed to have limited computational capabilities and constrained energy resources. However, we assume that they are capable of generating and managing cryptographic keys. We also assume that signal transmission is the major component of energy expenditure and therefore ignore any energy cost due to computation and information processing [1]. We further assume that omnidirectional antennas are used for transmission and reception of the signal.

We assume that the network has been successfully initialized, and initial cryptographic quantities (pair-wise trust establishment) have been distributed. Several novel approaches that address the critical problem of secure initialization in ad hoc networks with energy limitations, have been recently presented in [11], [12], [13].

IV. Routing-Aware Key Distribution

A. Formulation of the routing-aware key distribution problem

A member leave requires a significantly larger number of re-key messages than a member join [6], [7]. Although a member leave adds the same bandwidth overhead to the network (in a balanced key structure), the energy overhead depends on the underlying routing tree and key distribution tree [14]. In this paper we explicitly express the key update energy according to the multicast routing tree R and the key distribution tree T.

We assume that the probability of each member leaving the multicast group is uniform, i.e., members have equal probability of leaving the multicast group. For simplicity, we assume that $N = d^r,\ r \in \mathbb{Z}^+$. We denote as $\tilde{E}_{M_i}(R,T)$, the energy for re-keying after the member on the i^{th} leaf of the key tree leaves the multicast group and as $E_{TL}(R,T)$, the total energy expenditure after each member leaves the multicast group. For expressing those quantities we denote as $E_{S_{i.j}(T)}(R)$, the energy for transmitting a key from the GC to all members of the set $S_{i.j}(T)$, according to the routing tree R (for simplicity $S_{i.j} \equiv S_{i.j}(T)$ and $E_{S_{i.j}} \equiv E_{S_{i.j}(T)}(R)$). For the sake of illustration we first consider a binary tree with eight nodes.

Assume that M_1 in Figure 1(a) is leaving the multicast group. The key updates shown in Figure 1(b) need to be sent to valid members. The total energy expenditure for sending the re-key update messages is:

$$\begin{aligned}\tilde{E}_{M_1}(R,T) &= E_{S_{3.2}} + E_{S_{2.2}} + E_{S_{1.2}} + E_{S_{2.1}\setminus M_1} \\ &\quad + E_{S_{1.1}\setminus M_1} \qquad (1)\\ &= \sum_{i=1}^{3} E_{S_{i.2}} + \sum_{i=1}^{2} E_{S_{i.1}\setminus M_1} \qquad (2)\end{aligned}$$

where we denote as $S_{i.j}\setminus M_i$, the exclusion of M_i from set $S_{i.j}$. The term $E_{S_{3.2}}$ is due to the unicast transmission of $\{K'_{2.1}\}_{K_{3.2}}$ to M_2. The term $E_{S_{2.2}}$ is due to the multicast transmission of $\{K'_{1.1}\}_{K_{2.2}}$ to M_3, M_4. Similarly, the rest of the terms follow. The total energy for re-keying after each member leaves the multicast group is:

$$\begin{aligned}E_{TL}(R,T) &= \sum_{i=1}^{8} \tilde{E}_{M_i}(R,T) \\ &= \sum_{i=1}^{8} E_{S_{3.i}} + 2\sum_{i=1}^{4} E_{S_{2.i}} + 4\sum_{i=1}^{2} E_{S_{1.i}} + \\ &\quad \sum_{j=1}^{2}\sum_{k=1}^{4} E_{S_{1.j}\setminus S_{1.j}(k)} + \sum_{j=1}^{4}\sum_{k=1}^{2} E_{S_{2.j}\setminus S_{2.j}(k)} \\ &= \sum_{i=1}^{3} 2^{3-i}\sum_{j=1}^{2^i} E_{S_{i.j}} + \sum_{i=1}^{2}\sum_{j=1}^{2^i}\sum_{k=1}^{|S_{i.j}|} E_{S_{i.j}\setminus S_{i.j}(k)}\end{aligned}$$

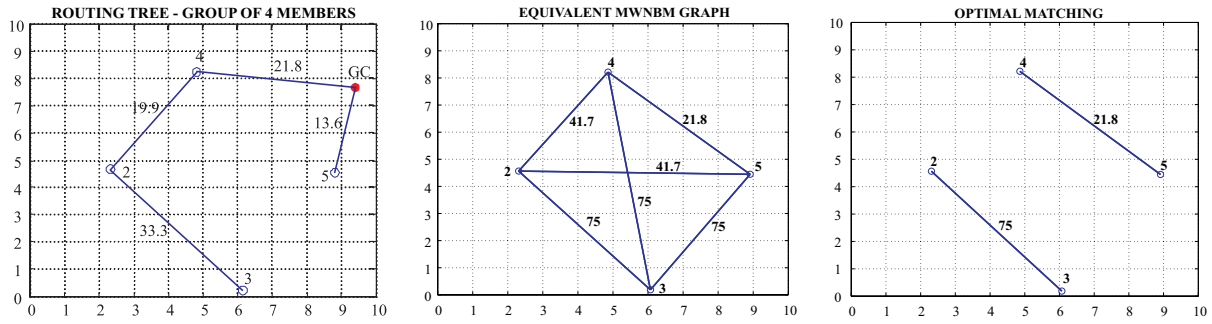
where $|S_{i.j}|$, denotes the size of the set $S_{i.j}$ and $S_{i.j}(k)$, denotes the k^{th} element of set $S_{i.j}$. Generalizing (2) to a d-ary key tree with N group members leads to:

$$\begin{aligned}\tilde{E}_{M_1}(R,T) &= \sum_{j=2}^{d}(E_{S_{h.j}} + E_{S_{(h-1).j}} + \ldots + E_{S_{1.j}}) \\ &\quad + E_{S_{(h-1).1}\setminus M_1} + \ldots + E_{S_{1.1}\setminus M_1} \\ &= \sum_{i=1}^{h}\sum_{j=2}^{d} E_{S_{i.j}} + \sum_{i=1}^{h-1} E_{S_{i.1}\setminus M_i} \qquad (3)\end{aligned}$$

The total energy for re-keying after each member leaves the multicast group in its general form is expressed as:

$$\begin{aligned}E_{TL}(R,T) &= \sum_{i=1}^{N} \tilde{E}_{M_i}(R,T) \\ &= (d-1)\sum_{i=1}^{N} E_{S_{h.i}} + (d-1)d\sum_{i=1}^{N/d} E_{S_{(h-1).i}} \\ &\quad + \ldots + (d-1)d^{(h-1)}\sum_{i=1}^{d} E_{S_{1.i}} \\ &\quad + \sum_{j=1}^{d^{(h-1)}}\sum_{k=1}^{|S_{(h-1).j}|} E_{S_{(h-1).j}\setminus S_{(h-1).j}(k)} \\ &\quad + \ldots + \sum_{j=1}^{d}\sum_{k=1}^{|S_{1.j}|} E_{S_{1.j}\setminus S_{1.j}(k)} \\ &= (d-1)\left(\sum_{i=1}^{h} d^{(h-i)}\sum_{j=1}^{d^i} E_{S_{i.j}}\right) \\ &\quad + \sum_{i=1}^{h-1}\sum_{j=1}^{d^i}\sum_{k=1}^{|S_{i.j}|} E_{S_{i.j}\setminus S_{i.j}(k)} \qquad (4)\end{aligned}$$

Hence the average energy required for re-keying after a member leave is $E_{AVE}(R,T) = E_{TL}(R,T)/N$. We observe that the average update energy depends upon the routing tree R and the key distribution tree T, i.e. the members' position on the leaves of the key distribution tree. We do not attempt to minimize $E_{AVE}(R,T)$ with respect to R, since R is optimized



(a) (b) (c)

Fig. 2. (a) An ad hoc network of 4 multicast members plus the GC. (b) The fully connected MWNBM graph $G(V, A)$. (c) The optimal solution for the MWNBM graph of (b). (d) The equivalent optimal key distribution tree.

MWNBM problem.	$\rightarrow$	Optimal sub-grouping of two members problem.
Set of vertices V.	$\rightarrow$	Set of multicast members $S_0(T)$.
Weight of edge $w(\epsilon)$.	$\rightarrow$	Energy expenditure for transmitting a message from the the GC to the members connected by edge $\epsilon \in A$
Optimum matching M for a fully connected graph $G(V, A)$	$\rightarrow$	Minimum energy expenditure for sending a message to sub-groups of two members $S_{h-1.i}(T),\ i = 1 \ldots \frac{N}{2}$.
$M^* = \arg\min_M \sum_{\epsilon \in M} w(\epsilon)$	$\rightarrow$	$T^* = \arg\min_T \sum_{i=1}^{N/2} E_{S_{(h-1).i}}$

TABLE I

EQUIVALENCE OF THE MWNBM PROBLEM WITH THE OPTIMAL SUB-GROUPING OF TWO MEMBERS PROBLEM.

to deliver the traffic stream to the multicast members. Instead, we are interested in selecting the optimal tree T^* that minimizes $E_{AVE}(R, T)$ given that routing is provided by the network layer.

$$T^* = \arg\min_T E_{AVE}(R, T) \tag{5}$$

We now investigate the solution approach to this formulation.

B. Complexity of the optimal solution

Solving the minimization problem in (5) is equivalent to minimizing $E_{TL}(R, T)$ expressed in (4), given that the members leave the multicast group with the same probability. From (4), we observe that $E_{TL}(R, T)$ consists of all the unicast energies to every multicast member (which are independent of the key tree structure we employ), plus the energies required for transmitting a key to every subset holding keys at level $(h-1)$ (sub-groups of two members), plus the energies for sending keys to every subset holding keys at level $(h-2)$ (sub-groups of four members) and so forth up to level one. The term $E_{TL}(R, T)$ also includes transmissions of keys to subsets holding keys at every level of the key tree, excluding the evicted member.

We now show that even for a sub group consisting two members, the optimal energy-efficient solution for updating keys under member deletion does not scale with group size. The goal then is to optimally select subsets of two members (partitioning the multicast group into subsets of two members), so as to minimize the energy expenditure for sending a message to every subset in the average sense. We now show that the problem of finding an optimal strategy for pairing members so that the total energy for updating keys is minimized when each subgroup has only two members can be transformed into the problem of *Minimum Weight Non-Bipartite Matching* (MWNBM) [2] described below:

MWNBM– Let $G(V, A)$ be an undirected graph. A matching M in $G(V, A)$ is a collection of edges $M \subseteq A$ such that no two edges in M are incident. Let $w : A \rightarrow \Re^+$ be a function which assigns a weight to each of the edge ϵ of G. The weight $w(F)$ of a subset $F \subseteq A$ of the edges of G is defined as $w(F) := \sum_{\epsilon \in F} w(\epsilon)$. The minimum weight non-bipartite matching problem is to find a perfect matching [1], M in G such that $w(M)$ is minimum.

Mapping the two-member keying problem to MWNBM problem. In the problem of mapping two-members to the leaves of the tree, we are given a fully connected graph with edges connecting the nodes indicating the energies for reaching the nodes connecting the edges. We want to pick the edges such that the total edge weight is minimal and every node is paired with one and only one another node. Hence, finding the optimal matching M^* for the fully connected graph $G(V, A)$ is equivalent to finding the optimal key tree T^* that assigns the least energy to transmit one message to subsets consisting of two members $S_{(h-1).i},\ i = 1 \ldots N/2$. The table I presents the mapping in detail. We now illustrate it with an example.

In Figure 2(a) we show the routing tree of a four-member multicast group, plus the GC. In Figure 2(b) we show the fully connected graph $G(V, A)$ of the equivalent MWNBM problem, with the weights $w(\epsilon),\ \epsilon \in A$, corresponding to the energy required to transmit a message from the GC to the two members connected by the edge ϵ. In Figure 2(c) we show the optimal matching M^* for the graph in Figure 2(b). Based on

[1] A matching is perfect if every vertex is matched with only one other vertex.

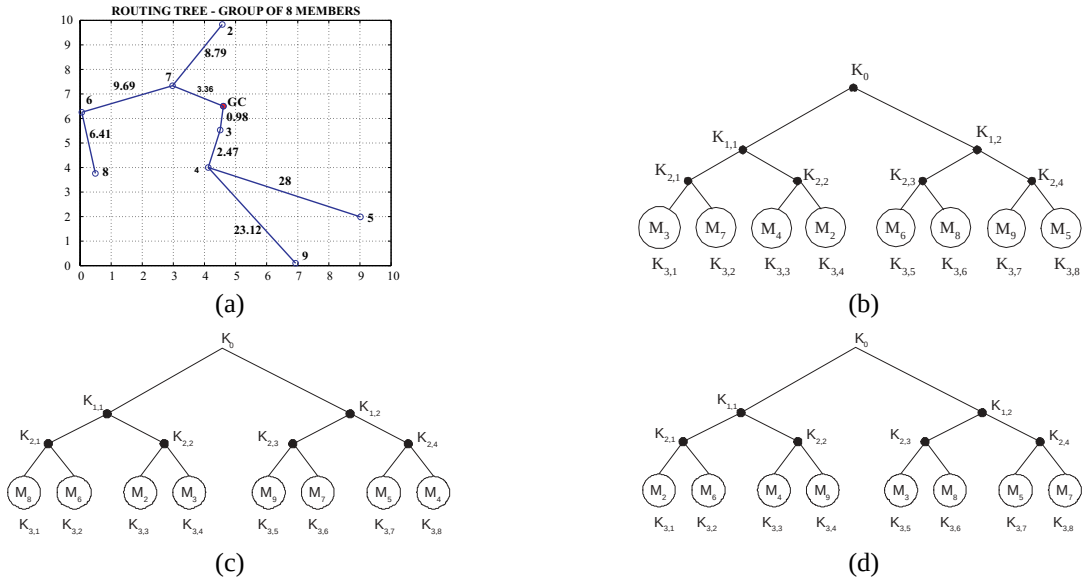


Fig. 3. (a) The routing paths of a wireless ad hoc network. (b) Key distribution tree built with the Routing-Aware key distribution algorithm. (c) Best possible Key distribution tree.

the Figure 2(c), we place the nodes $\{4, 5, 2, 3\}$ at the leaves of the key distribution tree, from left to right in that order.

Though several algorithms have been developed for finding the optimal solution of the MWNBM problem [2], [15], the most efficient technique [15] requires the use of sophisticated data structures and has complexity of $\mathcal{O}(N(m+Nlogn))$ where $|V| = N$ and $|A| = m$. Since our graph is fully connected, $m = \frac{N(N-1)}{2}$ and the complexity of the optimum solution becomes $\mathcal{O}(N^3)$. Since the key tree includes subgroups of various sizes, our observation implies that the complexity of constructing an optimal key tree will be at least as much as $\mathcal{O}(N^3)$. Hence, even the most efficient algorithm is not best suited for moderate to large multicast group sizes.

Using an example, we now show the negative result that obtaining the optimal solution for sub-groups of two members does not guarantee optimality for distributing keys to sub-groups of bigger size. The Figure 3(a) presents a routing tree of an ad hoc network. According to the routing tree in Figure 3(a), the optimal sub-group sets of size two are $\{3, 4\}, \{7, 2\}, \{6, 8\}, \{9, 5\}$ requiring total energy of 66.89 E.U. for sending one message to each group. The optimal sub-group sets of four elements are $\{2, 3, 6, 7\}, \{4, 5, 8, 9\}$ requiring 44.5 E.U. for sending one message to each group.

¿From this example, we observe that the optimal sub-group set of four $\{2, 3, 6, 7\}$, cannot be represented as the union of any of the optimal sub-group sets of two. This in turn implies that we cannot use MWNBM to iteratively construct the optimal key tree.

Characterization of the hardness of the original problem remains open.

C. A sub-optimal solution based on routing with low-complexity

The main idea behind the sub-optimal solution is based on the observation that in a secure multicast with single source having routing tree that is rooted at the source, the energy to reach a node from the source increases monotonically as the node distance from the source increases. Hence, if the routing is based on geometric distance, we can make use of it to arrange the nodes in an ascending order based on the energies required to reach them[2] We now describe the main idea.

Our sub-optimal solution relies on the multicast routing tree R for constructing an energy-efficient key distribution tree T. By accumulating information from the routing tables during the route path establishment, the GC can compute the energy $\mathcal{E}_i(R),\ i = 1..N$ required to unicast a message to each member of the multicast group.

Consider the nodes I and O and assume that $\mathcal{E}_I \leq \mathcal{E}_O$, where $\mathcal{E}_I$ is the energy to reach node I and $\mathcal{E}_O$ is the energy to reach node O. Then the energy expenditure for sending a message to both I and O is $\mathcal{E}_O$ if I and O share a common key, and $\mathcal{E}_O + \mathcal{E}_I$ if I and O do not share a common key. Hence, by assigning a common key to I and O we save $\mathcal{E}_I$ units of energy with maximum savings being achieved when $\mathcal{E}_I = \mathcal{E}_O$.

For example, in Figure 3(a), the node number five is relatively farther than node number nine from the source node. Hence, due to broadcast advantage of hte wireless medium, by transmitting to node five we will cover node nine. Assume that nodes five and nine need to receive a common enecrypted mesage. If they both share a common key, the source needs to perform only one transmission and the energy expenditure for sending a key to both five and nine is $E_{\{5,9\}} = 31.45$ Energy Units (EU). If they do not share a common key, the source needs to transmit two mesaages and the required energy is $E_{\{6,7\}} = 58.02$ EU.

If we sort all members according to $\mathcal{E}_i,\ i = 1..N$

[2]It is not difficult to construct counter examples that violate this statement. However, in most cases this statement is true for a routing scheme based on energy in wireless. Also, the existence of the counter examples is the reason for claiming the scheme as suboptimal.

in ascending order, we minimize the energy expenditure difference ($\mathcal{E}_{i+1} - \mathcal{E}_i$) between consecutive members and maximize the energy savings $\mathcal{E}_i$ if transmission to node O covers node I. Therefore, by assigning common keys to members differing the least in $\mathcal{E}_i$ (placing them under the same parent node in the key distribution tree) we achieve high energy savings. Based on this observation, we propose the placement of the multicast members to the leaves of the key distribution tree according to the ascending order of energy expenditure $\mathcal{E}_i$. We now present a sub-optimal Routing-Aware Key distribution scheme (RAwKey).

Routing-Aware Key Distribution Scheme (RAwKey)

Step 1:	Compute all $\mathcal{E}_i(R)$ from the GC to each member of the multicast group.
Step 2:	Sort $\mathcal{E} = \{\mathcal{E}_1, \mathcal{E}_2, ..., \mathcal{E}_N\}$ in ascending order.
Step 3:	Add members as leaf nodes to the key distribution tree, from left to right in the same order as $\mathcal{E}$.

Though this is not the optimal solution, its performance and implementation simplicity make it an extremely attractive method for key management in secure multicast communications for ad hoc networks.

D. Application of RAwKey to a sample network

We now illustrate the construct of the key tree for the nine-node network shown in Figure 3(a). The GC can communicate with each member of the multicast group by using the routing paths indicated. Sorting the energies for reaching each member of the multicast group gives $\mathcal{E}_{\{M_3\}} < \mathcal{E}_{\{M_7\}} < \mathcal{E}_{\{M_4\}} < \mathcal{E}_{\{M_2\}} < \mathcal{E}_{\{M_6\}} < \mathcal{E}_{\{M_8\}} < \mathcal{E}_{\{M_9\}} < \mathcal{E}_{\{M_5\}}$. The resulting key distribution tree is shown in Figure 3(b). The optimal key distribution tree, obtained by exhaustive searching, is shown in Figure 3(c). We can observe that the two trees are almost identical with only members M_4 and M_7 been interchanged. The worst possible tree, also obtained through exhaustive search is shown in Figure 3(d). The optimal possible tree has $E_{AVE}^{Optim}(R,T) = 62.7$ EU, the tree created with RAwKey has $E_{AVE}^{RAwKey}(R,T) = 63$ EU (0.5% worse than the optimal tree) and the worst possible tree has $E_{AVE}^{Worst}(R,T) = 78.3$ EU (24.9% worse than the optimal tree).

E. Complexity of RAwKey

RAwkey requires the computation of the unicast energies to reach every member of the multicast group sorted in ascending order. During the building of the multicast routing tree the GC can acquire the order by which nodes are added to the tree. In the case of SPR the order of adding nodes to the multicast tree is the same as sorting the unicast energies and no further steps are required.

When BIP or MST is used as a routing algorithm, the order by which nodes are added to the multicast tree is not the same as the ascending order of unicast energies. However, the set is almost ordered since nodes requiring less transmit power to be reached are in general added first to the routing tree. Hence, an efficient sorting algorithm for almost sorted data can significantly reduce the sorting time. Bubblesort [5] is known to have very good performance for almost sorted data with $\mathcal{O}(N)$ complexity in the best case (almost sorted sets). The EWMA uses MST as a base algorithm and hence, an almost ordered set can also be acquired.

V. Performance Evaluation

We performed our studies in randomly generated network topologies confined in a 10x10 region. Our network is assumed to be static. We assume that the energy required to transmit a key at a receiver located one distance unit away from the transmitter, is one energy unit.

A. Experiment 1: Evaluation of RAwKey algorithm

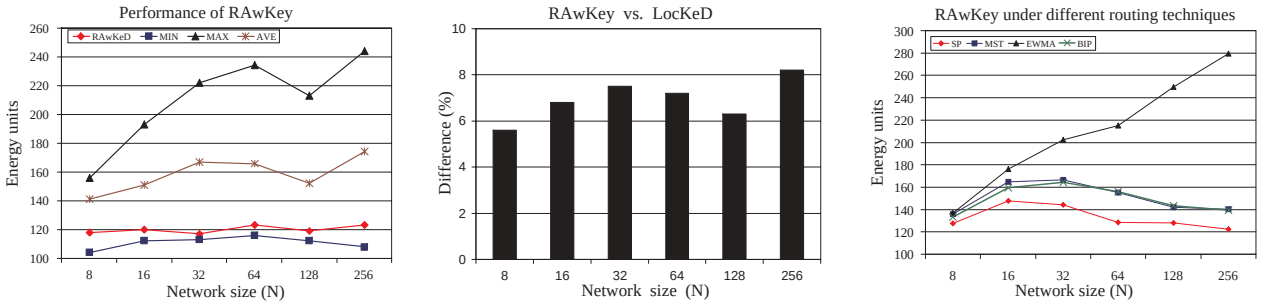
Since there is no algorithm to provide the optimal solution for the key distribution tree construction, we performed exhaustive search for $N = 8$. For larger group sizes $N = 16, 32, 64, 128, 256$, we generated for each network instance, 10,000 different key tree structures and compared the performance of RAwKey with the key tree that requires the minimum, maximum and median E_{AVE} out of the 10,000 tree structures. Further, we repeated the same comparison for 100 different network topologies and averaged the result.

In Figure 4(a), we observe that RAwKey yields significant savings compared to a tree structure that does not take into account the routing information. It has slightly worse performance compared to the best tree out of the 10,000 trees and gives significant savings compared to the median and worse possible tree. In Figure 4(b), we compare the performance of RAwKey with the location-aware key distribution scheme (LocKeD) we developed in [16]. We show the percentage difference ($\frac{E_{AVE}^{RAwKey} - E_{AVE}^{LocKeD}}{E_{AVE}^{RAwKey}}\%$) between RAwKey and LocKeD for different number of nodes. RAwKey outperforms LocKeD by 5.4-8.2%, since LocKeD may fail to capture the circularity of the broadcast advantage [16].

B. Experiment 2: Performance of RAwKey under different routing algorithms

In our second experiment we compared the performance of RAwKey under different routing algorithms and for different multicast group sizes. We generated random topologies and constructed the multicast routing tree using BIP [3], EWMA [4], MST [5] and SPR [5]. We applied RAwKey under the different routing algorithms and measured E_{AVE}. In Figure 4(c) we can observe that SPR gives the minimum re-key energy expenditure, BIP and MST have similar performance, while EWMA needs increasing energy for re-keying as the multicast group size grows.

By examining the type of routing trees resulting from the application of SPR, BIP, MST and EWMA, we can observe that SPR, BIP and MST tend to be multi-hop in contrast to EWMA that covers many nodes with one transmission. Although a



(a) (b) (c)

Fig. 4. (a) Performance of RAwKey for different N. (b) Comparison RAwKey with LocKeD for different N. (c) Comparison of the RAwKey under different routing algorithms.

single transmission is beneficial for broadcasting a message to all members of the multicast group and reducing the total transmit power, it proves inefficient when messages need to be transmitted to small sub-groups or even unicasted. Re-keying after a member leave involves many transmission to smaller groups than the whole multicast group. SPR is optimized for unicast transmissions and therefore delivers keys to single members with minimal energy expenditure. On the other hand, EWMA requires the most energy for unicasting, since it favors one-hop long range transmission to cover many nodes.

VI. Conclusion

We introduced a cross-layer design approach for key management in wireless multicast, that distributes cryptographic keys to valid group members in an energy-efficient way. By considering the physical and network layer, we formulated an optimization problem for minimizing the energy required for re-keying. We showed that the optimal solution is not scalable with group size N and developed a simple sub-optimal scheme that exploits available routing information. We call our scheme routing aware key distribution scheme (RAwKey). We illustrated the application of our scheme in binary trees and provided simulation results indicating that the performance of RAwKey is reasonable compared to the optimal. Finally, we studied RAwKey in conjunction with different underlying routing algorithms, and provided intuition behind performance variations that we observed. We argued that multicast routing algorithms with small unicast transmission energy, give smaller E_{AVE} due to the unicast and small group transmissions involved in re-keying. Proving the difficulty of the problem reamins open.

Acknowledgements

This work is supported in parts by the following grants: CARRER frant from NSF ANI-0093187, YIP from ARO under Cooperative Agreement DAAD19-02-1-0242 and the Collaborative Technology Alliance (CTA) from ARL under DAAD19-01-2- 0011. All statments and opinions are that of the authors and do not represent any position of the U.S government.

References

[1] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava, "Energy-Aware Wireless Microsensor Networks," IEEE Signal Processing Magazine, Vol. 19, Issue 2, pp:40–50, March 2002.

[2] J. Edmonds, "Maximum Matching and a Polyhedron with (0,1) vertices," in Journal of Research of the National Bureau of Standards, 69B, pp:125-130, April-June 1965.

[3] J.E. Wieselthier, G.D. Nguyen and A. Ephremides, "On the Construction of Energy Efficient Broadcast and Multicast Trees in Wireless Networks," in Proc. of IEEE INFOCOM 2000, Tel-Aviv, Israel, pp. 586-594.

[4] M. Cagalj, J.P. Hubaux and C. Enz, "Minimum-Energy Broadcast In All Wireless Networks: NP-Completeness and Distribution Issues," in Proc. of the 8^{th} ACM Annual International Conference on Mobile Computing and Networking, (MobiCom 2002), Atlanta, Georgia, September 2002.

[5] T. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein. Cagalj, *Intorduction to Algorithms*, Second Edition, MIT Press, Septempber 2001.

[6] D.M. Wallner, E.C. Harder and R.C. Agee, "Key Management for Multicast: Issues and Architectures," INTERNET DRAFT, Sep. 1998.

[7] C.K. Wong, M. Gouda and S. Lam, "Secure Group Communications Using Key Graphs," IEEE/ACM Trans. On Networking Vol.8, No.1, pp. 16-31, Feb. 2000.

[8] D. Balenson, D. McGrew and A. Sherman, "Key management for large dynamic groups: One-way Function trees and amortized Initialization," INTERNET DRAFT, Feb. 1999.

[9] A. Perrig, D. Song and D. Tygar, "ELK, a new protocol for efficient large-group key distribution," In Proc. of the IEEE Security and Privacy Symposium 2001, May 2001.

[10] F. Li and I. Nikolaidis, "On Minimum-Energy Broadcasting in All-Wireless Networks," in Proc. of the 26^{th} Annual IEEE Conference On Local Computer Networks (LCN 2001), Tampa, Florida, November 2001.

[11] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," In Security Protocols, 7^{th} International Workshop, 1999.

[12] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," In Proc. of the 9^{th} ACM Conference on Computer and Communications Security Washington D.C., USA, November 2002.

[13] H. Chan, A. Perrig and D. Song, "Random Key Predistribution Schemes for Sensor Networks," in IEEE Symposium on Security and Privacy, California, USA, May 2003.

[14] L. Lazos and R. Poovendran, "Secure Broadcast in Energy-Aware Wireless Sensor Networks," IEEE International Symposium on Advances in Wireless Communications (ISWC'02), Victoria, BC, Canada, September 2002.

[15] H. Gabow, "Data Structures for Weighted Matching and Nearest Common Ansestors with Linking," in Proc. of the First Annual ACM SIAM Symposium on Discrete Algorithms (SODA '90), pp:434-443, San Francisco, CA, USA, Jan 1990.

[16] L. Lazos and R. Poovendran, "Energy-Aware Secure Multicast Communication in Ad-hoc Networks Using Geographic Location Information," in Proc. of IEEE ICASSP 2003, Hong Kong, China, 2003.