SECURE BROADCAST IN ENERGY-AWARE WIRELESS SENSOR NETWORKS

Loukas Lazos, Radha Poovendran
Network Security and Cryptography Laboratory
University of Washington, Seattle, WA 98195
radha@ee.washington.edu, llazos@u.washington.edu

Abstract — **We consider the problem of securing multicast communications in an energy-constrained ad-hoc network environment. We show that existing efficient key distribution techniques for wired networks that rely on logical hierarchies are extremely energy inefficient for energy-constrained wireless ad-hoc networks. We also show that the joint consideration of routing and physical layer algorithms is critical for developing energy-efficient key distribution. We then formulate the correct problem and show that solution is hard to compute. We present a greedy, routing-aware key-distribution algorithm that is easy to compute[*].**

I. INTRODUCTION

Multicast communications model reduces the sender as well as the network management overhead when identical data has to be sent to a group of receivers. Many applications that make use of single-sender-multiple-receiver communication model can benefit from multicast mode. In order to ensure that only the valid members have access to the communication channel, the multicast communication is secured using cryptography [1]. The use of symmetric key cryptography allows the sender to perform one encryption and every user to perform one decryption per message, thus reducing the computational overhead. However, use of single key requires that the encrypting key is updated each time a group member joins or leaves to ensure the forward as well as backward traffic protection. Since every member holds the data encryption key, when a member leaves the group, a secure channel to reach the remaining valid members to update the data encryption key is required. Hence, the group has to have additional keys called Key Encrypting Keys (KEK) [1].

The key management problem is to ensure that only the valid members have the keys at any time. Developing efficient algorithms to allocate KEK to members is the key distribution problem. In case of wired networks, the rooted tree based hierarchical key distribution schemes are known to be optimal [1,4]. In [2], these results were directly used for energy-constrained sensor networks. However, as we show in this paper, such models are not energy-efficient. We present the formulation and results below.

II. WIRELESS AD-HOC NETWORK ENVIRONMENT

We assume that omni-directional antennas are used for transmission and reception of the signal. The required power P_d for reaching a receiver at a distance d is proportional to the γ^{th} power of that distance with $2 \le \gamma \le 4$. Assuming the proportionality constant to be one, we have $P_d=d^{\gamma}$.

We now demonstrate how transmission power (a quantity defined in the physical layer), affects the way the routing procedure is realized at the network layer. The wireless nature of the medium along with the omni-directional antennas, offer the unique characteristic of the *broadcast advantage* [3]. In figure 1(a), sender S transmits a message to node M_1, located at the boundary of the sphere. All nodes that lie within the sphere of radius $|SM_1|$ receive the message for "free".

We now show the impact of this physical layer property on the routing decision. In figure 1(b), assume that $d_2>d_1$ and that the sender S needs to transmit an identical message to nodes M_1 and M_2. Simple strategy would be to use unicast transmissions requiring a total energy expenditure of $(d_1^{\gamma}+d_2^{\gamma})$. However, broadcast nature of the wireless medium can reduce this expenditure as shown below.

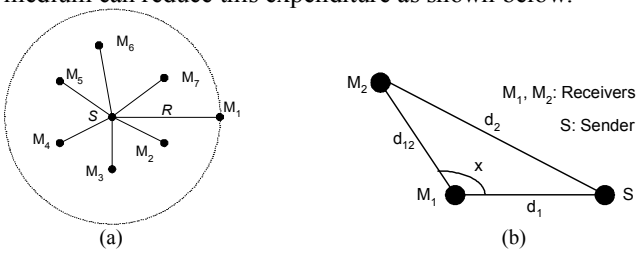

Fig. 1. (a) Broadcast Advantage for members M_1-M_7. (b) S transmits an identical message to both receivers

The sender can choose between one of the two following strategies: (a) transmit to M_1 and let M_1 relay the message to M_2. (b) transmit to M_2 and let M_1 receive the message for free, since $d_2>d_1$ (due to broadcast). This leads to the following rule: if $d_2^{\gamma}>(d_1^{\gamma}+d_{12}^{\gamma})$ then the sender chooses the strategy (a), otherwise strategy (b) is preferred.

III. IMPACT OF PHYSICAL AND NETWORK LAYER ON THE EFFICIENCY OF THE KEY DISTRIBUTION SCHEMES

We now demonstrate the need for routing-aware key distribution. In figure 2, we represent a wireless network of 7 nodes, with one of them being the sender denoted *GC*, and two intermediate nodes R_1, R_2 relaying traffic to four receiving nodes M_1-M_4, which form a multicast group. The energy required for sending a message from the *GC* to the two relay nodes is set to one unit and the energy required for sending a message from the relay nodes to the receiving nodes is also set to one unit. Hence, the *GC* need only to perform one broadcast to reach R_1, R_2 and, relay nodes R_1, R_2 each need perform one broadcast to reach $\{M_1, M_2\}$ and $\{M_3, M_4\}$ respectively.

Figure 3 presents two different key distribution strategies for the multicast group in figure 2. The one in figure 3(a) is built according to the available routing information, while the one in 3(b) is a result of a random placement of the members into the leaves of the tree. As a quick refresher [2], a member is assigned keys that are along the path traced from the leaf node to the root. For example, M_1 is assigned keys $\{K_0, K_{1,1}, K_{2,1}\}$. All the nodes share the key K_0.

[*] This work is funded by ARO grant DAAD19-02-1-0242

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Secure Broadcast in Energy-Aware Wireless Sensor 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

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**2**	

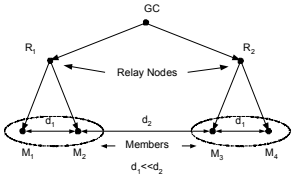

Fig. 2

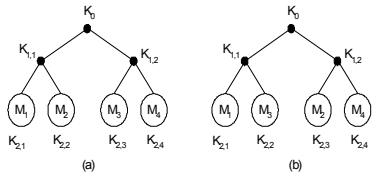

Fig. 3

Fig. 2. Routing tree of an energy constrained wireless network Fig. 3. (a) A hierarchical tree based key distribution scheme based on routing. (b) A logical hierarchical tree based key distribution scheme.

Let's assume that key K_0 has been compromised and needs to be replaced by the new key K_0'. For scheme in figure 3(a), the *GC* generates encrypted messages $\{K_0'\}_{K_{1,1}}$ and $\{K_0'\}_{K_{1,2}}$ and transmits them to relay nodes R_1 and R_2 respectively. Node R_1 performs one transmission to M_1, M_2 and R_2 performs one transmission to M_3, M_4. The total energy expenditure is four energy units. For scheme in figure 3(b), the *GC* transmits two messages to both R_1, R_2. Both R_1 *and* R_2 need to transmit twice to reach nodes M_1, M_3 and M_2, M_4, since nodes that share common keys cannot be reached with a single transmission. The scheme in figure 3(b) requires 8 energy units. *Hence, for this example, joint consideration of the network and physical layer information in the realization of the key distribution scheme leads to energy savings of 50%*. In larger networks with variable distances between nodes the energy savings can be even more significant. *Hence, the secure broadcast in energy-constrained wireless networks needs to be routing-aware.*

IV. Routing-Aware Key Distribution Scheme

We showed that the joint consideration of layer 2 and 3 is important in designing secure broadcast in ad-hoc networks. In this section we present a systematic approach based on the routing procedure for constructing an energy efficient key distribution tree. We make use of the routing information and try to design an energy-efficient key distribution scheme for secure broadcast.

We define the following quantities:

- N : multicast group size
- T : key distribution tree
- b_k^m (T): energy required to reach a set of members (this set or cluster is denoted by k) according to the established routing tree (broadcasting to those members) at level m of the tree T.
- $E_{TOTAL,m}(T)$*:* Total energy required to update all *keys* at level m of the tree T.
- $E_{TOTAL}(T)$ *:* Total energy required for updating all *keys* of the tree T.

Without loss of generality (more for clarity), we try to construct a binary tree with N leafs. Extension to a d-ary tree is straightforward. The depth of the binary tree is equal to $h = \lceil \log_2 N \rceil$. At level m of the key distribution tree, the total energy required for updating all *keys* is given by:

$$E_{TOTAL,m}(T) = \sum_{k=1}^{2^m} b_k^m(T) \qquad (1)$$

The total levels are equal to *(h-1)* since leaf keys do not need to be updated. The total energy required for updating *keys* at all levels is

$$E_{TOTAL}(T) = \sum_{m=0}^{h-1} E_{TOTAL,m}(T) = \sum_{m=0}^{h-1}\sum_{k=1}^{2^n} b_k^m(T) \qquad (2)$$

Given N nodes, we impose a balanced tree structure to allow the efficient delivery of data to subgroups of the global multicast communication group. The equivalent optimization problem is

$$T^* = \arg\min_T \sum_{m=0}^{h-1}\sum_{k=1}^{2^m} b_k^m(T) \qquad (3)$$

where T^* is the optimum tree structure that minimizes the energy required for a re-key operation. *It can be shown that the search space of such trees grows exponentially with group size. Hence, a heuristic solution is needed.* We propose a sub-optimal greedy method for finding an energy efficient key tree. We do this by choosing the cluster that requires the smallest amount of energy for key update. The clusters that are created at every level are fixed and act as a constraint to the upper level cluster formation.

Greedy Routing-Aware Key Distribution Algorithm

***Level h-1*:** At the leaf level, each cluster consists of two members. Using the available routing information we compute the required energy for updating all *N(N-1)/2* possible clusters of two members. We greedily pick *N/2* clusters. Our greedy algorithm consists of three steps: (1) arrange all pairs in ascending order of energy expenditure, (2) pick the cluster with smallest energy, (3) erase all clusters containing a node that was already selected, for the remaining clusters, repeat steps (2) and (3) till all members are selected.

Arbitrary level m (m=h-1;m>=1;m--): The clusters formed at level (m+1) are treated as single nodes (or leafs) for the formation of clusters at level m. The greedy algorithm is applied to $\frac{N}{2^m}\left(\frac{N}{2^{m-1}}-1\right)$ clusters and $N/2^m$ clusters are formed.

V. Conclusion

We showed that the secure broadcast in ad-hoc networks needs to jointly consider the physical and network layer algorithms to be energy-efficient. In particular, we showed that the results [1] do not generalize to ad-hoc networks. Recent past work had implied this generalization was feasible [2]. We also presented a routing-aware formulation and a greedy solution to it.

References

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

[2] D. Carman, P. Kruus, B. Matt, "*Constraints and Approaches for Distributed Sensor Network Security", NAI* Labs Technical Report #00-010 September 2000.

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

[4] R. Poovendran, "*An Information Theoretic Approach for Design and Analysis of Rooted Tree Based Secure Multicast Schemes*", IEEE Trans. Information Theory, Vol. 47, pp.2824-2834, November 2001.