SCOPE AND REQUIREMENTS OF A KEY MANAGEMENT FRAMEWORK FOR A MULTIPLE-GROUPS WIRELESS NETWORK

ALLA VENKA REDDY[1],KOPPALA ASHOK KUMAR[2],
ASSISTANT PROFESSOR[1],[2],
DEPARTMENT OF ECE
PBR VISVODAYA INSTITUTE OF TECHNOLOGY AND SCIENCE::KAVALI

ABSTRACT

Wireless sensor network security is a major area of research and development interest (WSN). However, modern security systems often need extensive iterations and several sophisticated encryption stages, which ultimately compromises service quality. Safe and reliable group communication is the foundation of many WSN uses. This study proposes a system for safe group key management that allows for numerous groups to exist at once. We demonstrate that the scheme's key-based group management can efficiently handle membership change events while saving on both memory and communication costs. It also provides the parameters and expectations for the communications sent inside and across groups.

KEYWORDS:

Collective Master Key, Secure group communication, key management, sensing node, and key tree

INTRODUCTION

A wireless sensor network consists of a collection of sensor nodes that have limited resources (battery life, processing speed, memory, etc.). The advent of Wireless Sensor Network (WSN) ushers in a plethora of novel concepts and developments. There are a plethora of potential uses and options available to us today. Healthcare, wearables, smart environment sensors, agricultural sensors, and military hardware are all examples of crucial areas where such technologies might be put to use. With the information they gather, these gadgets and sensors hope to provide a wealth of useful outcomes. However, the computational and processing power of such inexpensive devices is severely constrained. Therefore, a remote unit with computing capabilities to carry out such a procedure is required to address this challenge. In addition, the gadgets are compact and feature a little battery (e.g., batteries). As a result, they need to be energy efficient so that they can monitor and collect data with little drain on their batteries. Multiple aspects of the network, including its topology, device design, data collection system, and optimum security measures, contribute to the network's overall ability to save energy and transmit data more efficiently. More than a decade has been devoted to the pursuit of secure group communication, and several solutions have been presented throughout that time. In this piece, we'll go over some of the most up-to-date research on key distribution mechanisms and secure group communication, both of which can be found in the usual research article format.

Principal Methods of Management

We provide a method for group key management that allows for various groups. There may be a maximum of m groups operating at once, and each group consists of n sensing nodes. There is a total of n nodes (designated by the numbers s1, s2, etc.) and m groups (designated by the numbers G1, G2, etc.). Each group Gi, where I = 1, 2, m, has its own tree of logic built up. A group Gi's tree height is log2k if there are k (k n) nodes, where k is the number of sensing nodes in Gi. The core node is responsible for keeping the tree alive. For each class, it generates its own key tree. All of the sensors communicate with the master node using a secret key that is only known to itself. At the very top of the hierarchy sits the group key (GK), which is shared only among the members of the group for secure communication. Secondary keys are those that are related with a subgroup, which is formed when an inner node has two child nodes. Depending on whether the node has two children or one child, the key is labelled kin for j=1,2...m or kip-l. If it is the parent of the subtree whose leftmost child is is and whose rightmost child is so, then its key is kin; otherwise, it is kip-l (left or right). The level number is l, and kp is the node that is the leftmost or rightmost child of this subtree. The new group key is encrypted using secondary keys (keys along the way other than the group key and private key). The phases of group construction, key computation, and distribution are discussed next.

The range of the proposal Our Group Key Management Framework (KGMF) standard covers the following areas:

Infrastructure-based setting. The framework utilises a cellular networking environment based on fundamental cellular topologies.

Key management in a group setting. Our solution is narrowly tailored to the KGMF, whose overarching objective is to provide all communicating entities with the appropriate cryptographic keys and a way

to distribute these keys for the purpose of group communication while also providing essential security support.

Updates and distributions of keys are also included. The main concerns of the framework are key distribution and key updates, both of which are part of key management (or, re-keying). Every one of these tasks is critical and must be executed in a safe and sound way in accordance with the specifications of the multicast application in use.

Multicast application types Depending on whether or whether one or more senders transmit data traffic to many receivers (group members) in a multicast group communication, we may classify the multicast applications as either one-to-many or many-to-many interactions. Given that the proposal's focus is on key management rather than actual data transport, it doesn't matter what kind of multicast application is already in place.

Generalized representation. The suggested framework for group communication in Wireless Networks is defined at a high enough level of abstraction to be readily made interoperable with current network protocols, as well as application-layer security mechanisms.

DESIGN ARCHITECTURE

Here, we propose the architecture that we will use for our framework. We first determine the aspects that influenced our design decision. Design Influence

Domains and Areas:

We will adopt the notion of domains and areas as the main structural components in the framework architecture. This idea facilitates scalable and efficient distribution of keys to all group members, as group members are defined to exist in individual areas that are locally managed by a trusted entity.

Subgroups:

By placing group members in individual areas, we can associate them with the concept of subgroups. By doing so, we seek to overcome scalability problems that may occur whenever there is a change in group membership. When a new member joins (or an existing member leaves) a multicast group, it joins (or leaves) its local area and does not affect the other subgroups (in other areas) in the domain.

Symmetric Cryptography:

We follow previous KGMF proposals, and adopt symmetric cryptography in our proposal. This is primarily due to reasons pertaining to the nature of the wireless mobile environments that our framework.

Key Hierarchies:

Hierarchies of keys are very useful for group communication in Wireless Networks where group members may move between areas that may have their own security requirements. Further, we describe how each of these fits into our KGMF. The main controlling entities in both domain and area(s) are the following:

Master Key Manager (MKM).

At the domain level, a MKM is defined to exist, whose main responsibility is generating, distributing, storing and deleting all keying materials that may be required. We also assume that the MKM plays the role of group controller, which includes managing group policies, group membership, re-keying events and security policies.

The MKM's main roles are:

- Main key manager of a domain
- Collaborating with other key managers (at the area level) to provide secure and efficient key management services within a domain
- Generating and distributing cryptographic keys to all Local key managers in the domain governing all re-keying events that may occur during the lifetime of a multicast group
- Working closely with Local key managers to govern host mobility.

Local Key Manager (LKM)

One LKM is defined for each area. The main responsibility of an LKM is running the key management aspects relating to an area, including those of the group members residing within that area. Operating under the MKM's

jurisdiction, an LKM is responsible for any re-keying event that may occur at the area level. The LKM also works closely with the MKM to manage host mobility that may occur across the domain. The LKM's main roles are:

- Main key manager of an area
- Assisting the MKM to provide secure and efficient key management services to group members in areas
- Generating and distributing cryptographic keys to all group members residing in an area

• Governing re-keying events at the area level, operating under the MKM's jurisdiction

• Working closely with the MKM and other LKMs to govern host mobility.

Domain(s) and Area(s)

Here, we look more closely at the domain(s) and area(s) within the architecture. We also discuss interactions across various domains, when such cross-domain group communication is allowed theconcept of domains and areas allows for an easily controlled setting in which groups may communicate with one another, which is especially useful for centralised key management. In our approach, a domain's definition might be either logical or physical. In either case, the network is owned and maintained by a reliable organisation adhering to a unified set of standards, such as the Global System for Mobile Communications (GSM) operator (Lin and Chlamtac, 2001). Each of these subdomains is overseen by a Local Key Manager (LKM) who works closely with the Master Key Manager (MKM) in charge of the whole domain. Domain j is further subdivided into various sections labelled Area a through Area e, all of which might logically or physically overlap with one another, as shown in Figure 1. Given that there is only one MKM in charge of a given domain, it follows that all its constituent parts should be able to communicate with one another without issue. It is important for a group member to get security information (i.e. keys) connected with the new area before or during a migration from their local area to another area, even if the areas within the domain are utilising comparable systems for interoperability. As a corollary, host mobility in wireless networks may disperse a group's members across locations, each of which may impose its own set of constraints on the data those members may access. The following terms are used to distinguish between tasks in groups:

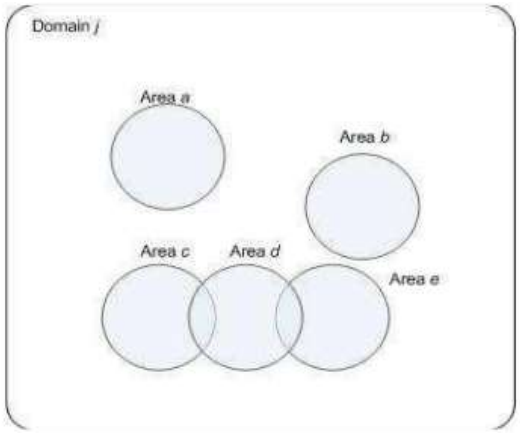

Figure 1: An Example Showing the Notion of Domain and Areas.

close-by places

The geographical region where hosts (possible group members) are initially exposed to a multicast broadcast is called the local area.

Map of Sighted Locations

When talking about locations in a domain that group members may or may not go to (during host mobility), we use the phrase "visited area."

Relationship Between Disciplines

We define the concept of cross-domain links here. If group actions from outside the local domain are allowed, this is helpful (for example, when a host or potential member wishes to join a multicast group that is managed by another domain). A cross-domain request is an example of this.

As for how to handle communication across domains, there are two options:

Involvement of a Middleman

Inter-domain communication may be handled in one of two ways. The first is to designate a dedicated component, such as a server or router, to handle all such interactions (if it occurs). If a user makes a request to join a multicast group and that group isn't located in their domain, the request is sent to the aforementioned entity. To connect these two separate spheres, this thing serves as a connecting node. Depending on its hardware and software, an intermediary host may support many inter-domain connections. The ideas in (Hardon et al., 2000a) and elsewhere are precursors to this intermediary entity (Hardon et al., 2000b). The necessity for a translation entity or router that can translate any cryptographic communications protected by foreign keys that are incomprehensible to the present domain is briefly discussed in (Hardjono et al., 2000a) and (Hardjono et al., 2000b).

Using MKMs as a reference for one another

One alternate method is to look for information on different MKMs using one another. Inter-domain requests in this situation are controlled by MKMs from both of the impacted domains. Let's say we're talking about domain I and domain j, and we abbreviate them as Di and Dj respectively. Each host has a Master key manager that controls its

membership in any multicast group outside of the host's local domain Di (the location of the host at the time of the request) (MKM). When a host request is made, the MKM communicates with the MKM in Dj to control it, including any security relationship exchange that may take place. Inter-domain communication can only be accomplished via the combined efforts of both MKMs.

Objects' Locations

Domain-level key management is supervised by an MKM, whereas local key management is supervised by a LKM. In Figures 4.2 and 4.3, we show how entities should be placed in two examples. As can be seen in Figure 2, below, there is a correlation between the i-th domain and the j-th area. We assume a sender and a receiver to stand in for the members of the multicast group, while MKM is the primary key manager of domain I and LKM is the key manager of area j, based on the example. There is a clean conceptual break between domain I and region j, as shown by the horizontal dotted line. All of the lines denoted by dotted arrows between the MKM and LKM, as well as between the LKM and the sender and the receiver, indicate control. channels that can be used to send control messages between the MKM and LKM. These messages may include confirmation of a successful re-key or an acknowledgment of a message's receipt. The single arrow from sender to receiver depicts the data channel of actual group communication that may occur after the exchange of keys and SA management between pairs of entities is shown by the two arrows.

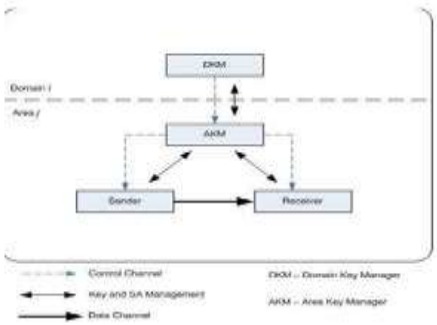

Figure 2: Placement of Entities in Domain I and Area j.

On the other hand, Figure 3 shows placement of group members M across a domain j, where distribution of members occurs throughout the areas as to e. The arrows denote the movement of group members between the areas.

CONCLUSIONS

Over the last several years, researchers have focused extensively on the problem of ensuring the safety of group conversations. Security services are required for Group Key Management Framework applications in WSN in order to provide safe group communication. When sending information between members of a group, it is usual practise to encrypt the data using a secret key known only to the members of the group. Thus, key management is a fundamental building block for establishing trust in distributed communication networks. In this research, we provide a Group Key Management Framework strategy for WSNs that support multiple groups. As a means of communication between ourselves, we have used a group key-based strategy.

REFERENCES

[1]. H.S.Annapurna and M.Siddappa, "Key management scheme for secure group communication in WSN with multiple groups", Computer Science & Information Technology (CS & IT), pp. 91–101, 2016.

[2]. N.Meghanathan, S. Boumerdassi, N. Chaki, D. Nagamalai, "Recent Trends in Network Security and Applications: Third International Conference", The Third International Conference on Network Security and Applications, 2010.

[3]. R.Shyamala, S. Valli, "Impact of Black hole and Rushing Attack on the Location-Based Routing Protocol for Wireless Sensor Networks", Advance in Computer & Inform, Technology, pp. 349-359, 2012.

[4]. T. Shimeall, J. Spring, "Introduction to Information Security: A Strategic-Based Approach", Newnes Compute, pp. 382, 2013.

[5]. J.Sen, "Security and privacy challenges in cognitive wireless sensor networks", arXiv preprint arXiv: 1302.2253, 2013.

[6]. G. Sharmaa, S. Balaa, A.K.Vermaa, "Security Frameworks for Wireless Sensor Networks-Review", 2nd International Conference on Communication, Computing & Security, SciVerse Science Direct, 2012.

[7]. C. Cheikhrouhou, A. Koubâa, G. Dini, and M. Abid, "RiSeG: a ring based secure group communication protocol for resource-constrained wireless sensor networks", Personal and Ubiquitous Computing, Vol. 15, No. 8, pp. 783- 797, 2011.

[8]. X. Wanga, P. Lia, Y. Suia, and H. Yanga, "A Hexagon-based Key Pre-distribution Scheme for Wireless Sensor Networks", Journal of Information & Computational Science, Vol. 11 (8), pp. 2479-2491, 2014.

[9]. M. Miettinen, N. Asokan, T.D.Nguyen, A-R.Sadeghi, and M. Sobhani, "Context-Based Zero-Interaction Pairing and Key Evolution for Advanced Personal Devices", In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 880-891, 2014.

[10]. J. Furtak, and J. Chudzikiewicz, "The concept of authentication in WSNs using TPM", Computer Science and Information Systems, Vol. 3, pp. 183–190, 2014.

[11]. W. Xi, X-Y. Li, C. Qian, J. Han, S. Tang, J. Zhao