IMPACT: International Journal of Research in Humanities, Arts and Literature (IMPACT: IJRHAL)
ISSN (P): 2347–4564; ISSN (E): 2321–8878
Vol. 7, Issue 3, Mar 2019, 601–612
© Impact Journals

KEY MANAGEMENT FRAMEWORK FOR WIRELESS NETWORK IN MULTIPLE GROUPS: SCOPE AND REQUIREMENTS

Dr. A. Singaravelan

Professor, Department of Computer Science, ESSM College of Arts and Science, Tiruvallur, Tamil Nadu , India.

Received: 14 Mar 2019 **Accepted:** 22 Mar 2019 **Published:** 31 Mar 2019

ABSTRACT

Security is one of the important challenges in the field of Wireless Sensor Network (WSN). But nowadays, majority of the security protocols involve massive iterations and complex steps of encryptions thereby giving up to degrade the quality of service. Many WSN applications are based on secure group communication. In this paper, here, we have proposed a method for secure group key management framework with simultaneous multiple groups. The scheme uses a key based on managing the groups and we show that membership change events can be handled with reduced memory and communication cost. It also offer the scope and requirements to the messages communicated within and among the groups.

KEYWORDS: *Group Key, Key Management, Sensing Node, Secure Group Communication, Key Tree*

INTRODUCTION

Wireless Sensor Network is a collection of sensor nodes with limited capabilities in terms of battery, computation, storage etc. Wireless Sensor Network (WSN) brings new ideas and innovations to our life. Today, we are surrounded by a wide range of applications and opportunities. For instance, healthcare, wearable devices, smart environment sensors, agriculture sensors and military devices are examples of such important applications. These devices and sensors aim to collect data to provide a numerous of valuable results. However, these low end devices come with very limited computation and processing capabilities. Therefore, to overcome this issue, there is a need for a remote unit with computation capability to perform such a process.

Furthermore, these devices are small and have limited internal power source (e.g., batteries). Thus, they need to be power efficient to reduce power consumption while monitoring and gathering data to maximize their battery life. In fact, power consumption and data transmission reduction are affected by several areas in the network, for instance network topology, device architecture, data gathering scheme and optimized security schemes.

The study towards secure group communication is more than a decade old and there are various techniques that have been introduced by the various researchers. This section discusses some of the recent studies found in standard research manuscript that focuses on i) secure group communication and ii) key distribution mechanism.

KEY MANAGEMENT METHODS

We propose a scheme for group key management with multiple groups. A group consists of n sensing nodes and there are at most m simultaneous groups that need to be established. The nodes are numbered s1, s2…sn and groups are numbered G1, G2… Gm. A logical tree in constructed for each group Gi, for i =1,2...m. The height of the tree for group Gi depends on the number of sensing nodes in Gi and it is log2k if there are k (k ≤ n) nodes in the tree. The tree is maintained by the central node. It constructs a separate key tree for each group. Each sensing node shares a private key with the central node which is used for confidential communication. The group key (GK) is at the root of the tree and is used for confidential communication with the group members. An interior node with two child nodes forms a subgroup and keys associated with the subgroup are called secondary keys. These keys are named either kij for j=1,2…m or kp-l depending on whether they have two child nodes or one child node. The key is named kij if it is the root of the subtree with leftmost child si and rightmost child sj and it is named kp-l if it is the root of the subtree with one child node (left or right). kp is the leftmost or rightmost child (whichever exists) of this subtree and l is the level number. Secondary keys (keys along the path excluding group key and private key) are used to encrypt new group key. Next we discuss group formation phase followed by computation and distribution of group key.

SCOPE OF PROPOSAL

Regarding the scope of our Group Key Management Framework(KGMF) specification, it is important to note the following:

- Infrastructure-based environment. The framework relies on an infrastructure based environment with a basic different cellular architectures as its networking platform.

- Group key management. Our proposal focuses solely on the KGMF, whose main goal is to provide fundamental security support by providing all communicating entities with the necessary cryptographic keys, and providing a means to distribute these keys for the purpose of group communication

- Key distributions and key updates. The aspects of key management that the framework is primarily concerned with are *key distribution* and *key updates (or, re-keying)*. Each of these is important and should be conducted in a proper and secure manner as required by the multicast application in place.

- Type of Multicast Applications. The multicast applications can be categorized as *one-to-many* or *many-to-many* relationships, depending on whether a single (or, many) sender(s) transmit data traffic to many receivers (group members) in the multicast group communication. Since the scope of the proposal is primarily concerned with key management and is not concerned with the real data communication, the type of multicast application in place does not matter and does not affect the proposal design.

- Generic model. The framework proposed is stated in sufficient abstraction that it can easily be made compatible with existing network protocols, as well as application-layer security protocols to allow for practical implementation for group communication in Wireless Networks.

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 multiple domain relationships, in the cases where inter-domain group communication is permitted. The notion of domain(s) and area(s) provides a means to have an administratively manageable environment for group communication to take place, most importantly for efficient key management. In our proposal, a *domain* can be logically or physically defined. Either way, it is controlled and managed by a trusted entity operating under one system, for instance the *Global System for Mobile Communications* (GSM) operator's network (Lin and Chlamtac, 2001).

The domain is further divided into a number of smaller manageable areas, each of which is managed by an LKM, operating closely with the MKM with regards to key management. We illustrate the notion of domain and areas in *Figure 1* where, Domain j is further divided into several areas labelled Area a to e, each of which can be logically or physically overlapping with one another. Since a domain is controlled by one MKM, all corresponding entities across a domain should be able to interface successfully with one another. Although areas within a domain may be using similar systems for interoperability, this does not change the fact that each area is unique and that a group member that moves from its local area to another area must obtain security information (i.e. keys) associated with that area prior to, or during, the move. Furthermore, in Wireless Networks host mobility may place group members in different areas, each of which has its own restriction on what information may or may not be accessed by the mobile members. We use the following definitions to differentiate areas during group operations:

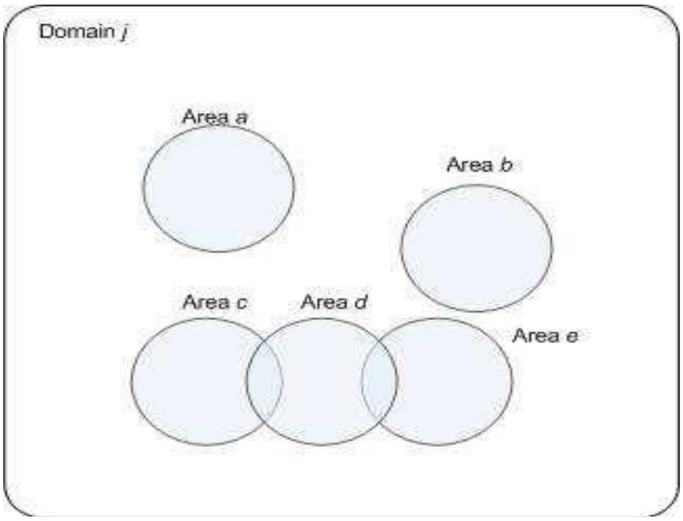

Figure 1: An Example Showing the Notion of Domain and Area.

- **Local Areas**

The term *local area* is used to refer to the area where hosts (potential group members) first join a multicast group.

- **Visited Areas**

The term *visited area* is used to refer to other areas in a domain, where group members may or may not *move to* (during host mobility) throughout the lifetime of their group membership.

Inter-Domain Relationship

In this section, we introduce the idea of *inter-domain* relationships. This is useful in cases where group operations originating from outside the local domain are permitted (for example, when a host or potential member wishes to join a multicast group that is managed by other domain). This kind of request is called a *cross-domain request*.

There are two approaches that can be adopted in dealing with inter-domain communication:

- **Use of an Intermediate Entity**

The first approach is to have a separate entity, which can be in the form of a server or a router, to deal with any inter-domain communication (if it occurs). For example, any request to join a multicast group that is not in the current domain where the request originates from is transferred to the aforementioned entity, which deals with the inter-domain requests. This entity thus acts as an intermediate node or a bridge between the two distinctive domains. An intermediate host may cater for two or more inter domains communications depending on its hardware or software capacity. This intermediate entity is similar to existing proposals in (Hardjono et al., 2000a) and (Hardjono et al., 2000b). Briefly, (Hardjono et al., 2000a) and (Hardjono et al., 2000b) discuss the need for a translation entity or a router that is able to translate any cryptographic messages protected by foreign keys that are unintelligible to the current domain.

- **Cross-Referencing between MKMs**

An alternative approach is the cross-referencing between MKMs. In this case, MKMs from both affected domains are the ones governing the inter domain requests. For example, let Di and Dj denote domain i and domain j. Any host who wishes to join a multicast group outside its local domain Di (the point of where it is residing at the time of the request), is managed by its Master key manager (MKM). The MKM then liaises with the MKM in Dj to govern the request, including any security relationship exchange that may occur during the course of the host request. Both MKMs need to collaborate in order to realize inter-domain communication.

Placement of Entities

A MKM oversees key management at the domain level, and an LKM oversees key management at the area level. We illustrate placement of entities in two instances in *Figure:4.2* and *Figure:4.3*.

Figure: 2 below shows placement of entities in domain i and area j. From the illustration, while MKM is the main key manager of domain i and LKM is the key manager of the area j, we assume there is a sender and a receiver to represent the group members of the multicast group in place. The horizontal dotted-line shows a logical division between domain i and area j. The *dotted-arrow* lines from MKM to LKM, as well as from LKM to both sender and receiver, show *control* *channels* which can be used by the MKM and LKM for transmitting control messages, such as notification on re-keying that has taken place, or acknowledgement of messages received.

While *double-arrow* lines show the exchange of key and SA management between pairs of entities, the *single-arrow* line from sender to receiver shows the data channel of real group communication which may take place after the exchange of key and SA management occurs.

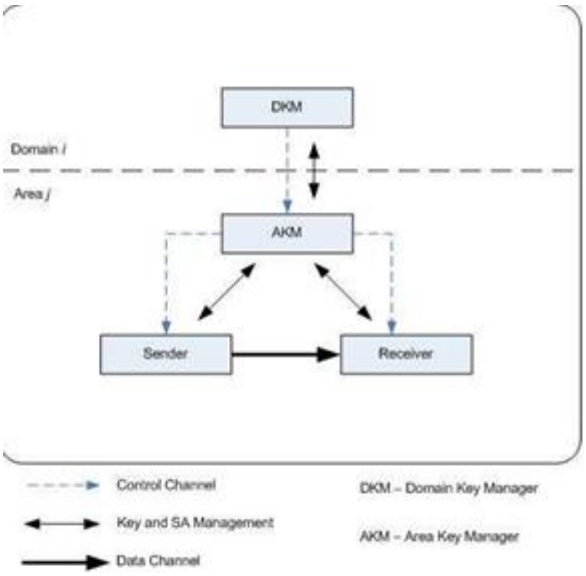

Figure 2: Placement of Entities in Domain i and Area j.

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

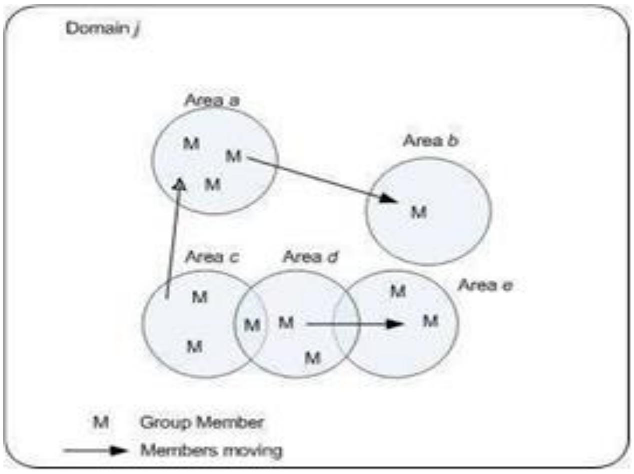

Figure 3: Placement of Group Members Throughout Areas.

Trust Relationships

The trust relationships often revolve around key managers, who are the main key distributors. In our framework, we assume that all key managers (MKM and LKMs) in a domain are trustworthy and reliable. All group members of multicast groups trust these key managers, particularly for providing secure key management services.

There are two levels of trust relationships:

- **At the Domain Level**

At the domain level, all LKMs trust the MKM as the primary key distributor, as well as the main group manager for various multicast groups operating in that domain.

- **At the Area Level**

At the area level, all group members (residing in that area) trust their LKM as the main reference point for security parameters needed for group communication.

Types of Key

In this section, we look at another of the fundamental components of the proposed architecture, namely the cryptographic keys. We base our framework on symmetric key cryptography because most mobile devices that operate in Wireless Networks exhibit special characteristics, which benefit from the computationally faster and less complex techniques offered by the symmetric approach. In the following sections, we look at the symmetric keys used in our framework, which are categorized into two main groups; *long-term* and *short-term* secret keys. We assume that all symmetric keys used are of an appropriate recommended length (at the time of writing we recommend 128 bits), allowing the use of standard algorithm such as AES (FIPS, 2001). We end this section by looking at the aspects of key management that we assume are in place and available for the purpose of group key management, and that we will thus not fully specify in the framework.

Long-Term Keys

Long-term keys are assumed to have been established prior to any host joining a multicast group. Entities in the framework use these keys to securely initiate secure group communications, including when disseminating short-term keys. There are three types of long-terms key in the framework; *Domain-Area keys*, *Domain keys* and *Area-Member keys*. The following subsections describe each key in turn, and their details are summarized in Table 4.1.

Table 1: Long-Term Keys and its Functions

Key	Generated by	Held by	Function
Domain-Area key	MKM	MKM,LKM	(a) Unique to MKM and a specific LKM. (b) Supports unicast communication between MKM and LKM. (c) Supports secure distribution of the domain key.
Domain key	MKM	MKM,LKM	(a) Common key for MKM and all LKMs. (b) Supports multicast communication amongst MKM and LKMs. (c) Supports secure distribution of the traffic key.
Area-Member key	MKM	MKM,LKM,M	(a) Unique to LKM and a specific M. (b) Supports unicast communication between LKM and M. (c) Supports secure distribution of the area key in an area.

- **Domain-Area Key, DAi−Key**

The Domain-Area key is the unique long-term key shared between the MKM and a specific LKM in a domain. More precisely, DAi−Key corresponds to the symmetric key shared between MKM and the Local key manager LKMi of area i.

This unique key is established with every LKM in the domain prior to any request to create multicast groups in the domain. Each key is generated and distributed by the MKM to every LKM by an appropriate secure means, We assume that the membership of all key managers in a domain is predetermined and fixed. Thus, each Domain-Area key is static and valid until the policy determines otherwise. Once a Domain-Area key expires (or is revoked), a new key must be generated and distributed to the affected LKM. The function of each Domain-Area key is restricted only to *unicast* communication between the MKM and a particular LKM.

- **Domain Key, D−Key**

The Domain key D−Key is the long-term key shared by all key managers (i.e. MKM and all LKMs) in a domain. Like the Domain-Area key, the domain key is established prior to any request to create multicast groups in the domain. D−Key is generated and distributed by the MKM to all LKMs via secure channels. One such channel is created by unicasting under the appropriate *Domain-Area* keys. Since the group membership of all key managers is static, D−Key is also fixed and valid until the policy determines otherwise. A new domain key must be generated and distributed to all LKMs to replace the old one on its expiry. Although D−Key is often used to assist secure distribution of other keys needed for group communication, it is also referred to as a *control key* because it can be used by the MKM to send control messages, such as to notify all LKMs in the domain of a new multicast group, re-keying events that are taking place, as well as any notification concerning host mobility.A desirable function of D−Key is that it provides a means for *multicast* transmission of messages among all key managers in a domain.

- **Area-Member Key, AiM−Key**

Another long-term key used is a unique Area-Member key shared between the LKM of an area and every group member residing in that particular area. More precisely, AiM−Key corresponds to a symmetric key shared between Local key manager LKMi and a group member M. This key is obtained during the first contact that a host (who soon will become a member of a multicast group) makes to the LKMof a particular area to register with a particular multicast group. We assume that the Area-Member key is established prior to any request to join the group, and is generated and sent by the MKM to a particular LKM, which then sends it to the group member M. More precisely, at the domain level, the MKM uses the Domain-Area key to secure the distribution of the Area-Member key to a particular LKM of an area. Then, at the area level an LKM uses a *secure means* to distribute the key to the group member M. Since group membership can be dynamic, we assume that the Area- Member key remains valid throughout the lifetime of a particular multicast group, or until the group member has ceased to be a member of that particular multicast group. Like the Domain-Area key, the function of each Area-Member key is restricted only to *unicast* communication between the LKM of an area and a group member of that area.

Short-Term Keys

Short-term symmetric keys are assumed to have been established after group members join multicast groups (or after the long-term secrets have been established). As group members are already in possession of long-term keys, these are often used to assist secure distribution of short-terms keys. There are three short-terms keys introduced in the framework; *traffic encryption keys, area keys* and *session mobility keys*. The following sections describe each type of key in turn, and at the end their details are summarized in Table 4.2.

Traffic Encryption Key, T−Key

The Traffic Encryption Key (or *traffic key*) T−Key is a short-term key shared by all group members of a particular multicast group in a domain. There is a unique traffic key for a specific multicast group. T−Key is generated and distributed by the MKM to all LKMs in the domain, which then in turn disseminate this key to all group members residing in their area. The establishment of the key takes place only after the first host creates (and joins) a multicast group. There are several options for securing the distribution of the traffic key to all group members in the domain. One option is for the MKM to use *unicast*, by protecting the key under each Domain-Area key and thus sending it to every LKM independently. At the area level, an LKM uses the same method using each Area-Member key. Another option is for the MKM to use *multicast* and send a single message containing the traffic key to all LKMs protected under the domain key D−Key. Each LKM in turn distributes the traffic key to all group members in the area. If all group members residing in the area belong to the same multicast group, LKM can send the traffic key by multicast using the area key A−Key (see next subsection). Otherwise, LKM will have to unicast to every member protected under the Area-Member key. The main function of the traffic key is to protect the real data in communication. The traffic key is valid throughout the lifetime of a multicast group, or until the policy determines otherwise. To replace a traffic key, a new traffic key must be generated and distributed to all group members in the domain.

Area Key, A−Key

The Area key is a short-term key unique to an area. Every area has a different A−Key. An area key is generated and distributed by the LKM of a particular area, and shared only by group members residing in that area. An area key is established with a group member after it joins a multicast group. The dissemination of the area key to all group members is done by the LKM via *unicast* methods using each Area-Member key.

The main purpose of having an area key, which is unique to an area, is:

- **To Securely Manage Host Mobility Across Areas in the Domain**

Without proper control, group members that are moving from one area to another may collect security information, including old keys not authorized to them. In addition, different areas may have different access control pertaining to their local information. By having adequate access control, one can prevent such security violations by unauthorized moving members.

- **To Provide Efficient and Scalable Re-Keying**

Unique area keys are useful for efficient re-keying and promote scalability, since group members within an area are managed under one unique key. Note that while group members of a multicast group can be dispersed across the domain due to host mobility, each group member may have in his possession a different set of area keys. The first area key that a host may possess is from the area where it resides the first time it joins a multicast group, in other words the *local area*. An area key is often used to assist secure multicast distribution of the traffic key to all group members in an area in a single transmission. An area key is assumed valid as long as there are members residing in that area, or until the policy determines otherwise.

- **Session Mobility Key, Sm−Keyiv**

The Session mobility key Sm−Keyiv is a short-term symmetric key shared between an LKMand a moving group member. More precisely, Sm−Keyiv is a session mobility key shared between an Local key manager LKMv and a group member Mi. This key is only used for host mobility and exchanged during the hand-off operation.

This key is established between a moving member and the LKM of a visited area prior to host mobility. The generation and initial distribution of this key is conducted by the MKM in a domain, then delivered to the group member via an LKM in the local area (where the member is currently residing). The same key is then delivered to the LKM of a visited area by the MKM. The delivery of the session mobility key must be done using secure channels. This key is used for any unicast communication that may occur between the LKM of the visited area and the mobile member throughout its residence period in that area. This includes the secure distribution of the visited area's area key to the mobile member.

In the case where a mobile member is moving to another area from its visited area, it then has to establish another session mobility key with another Local key manager of the area it is moving into. Unless policy determines otherwise, a group member may possess a session mobility key for every area that it visits throughout the lifetime of its group membership. This session mobility key is valid throughout the member's residing period in that area or until it ceases to be a member of the multicast group. The function of the session mobility key is restricted only to unicast communication between the LKM and a particular group member of a multicast group.

Table 2: Short-Term Keys and their Functions

Key	Generated by	Held by	Function
Traffic key	MKM	MKM,LKM,M	(a) Common key to all MS in a group. (b) Unique to a specific multicast group. (d) Secures the actual data communication.
Area key	LKM	LKM,M	(a) Unique to an area. (b) Supports multicast communication amongst LKM and all MS in a group. (c) Supports secure distribution of the traffic key to MS in a group.
Session Mobility key	MKM	MKM,LKM,M	(a) Unique to LKM and M. (b) Supports unicast communication between LKM and M. (c) Supports secure distribution of area key for host mobility.

Assumptions on Aspects of Key Management

We will focus on distribution and updating of (mainly short-term) cryptographic keys. Other operations are not treated here in detail because their provision can be achieved by generic solutions which are not specific to group communication. The following assumptions regarding key management operations are made:

- Key generation is conducted in a secure and proper manner by all key managers (MKM and LKMs) in a domain. We assume that key managers use recognized key generators to generate keys as randomly as possible.

- Long-term key distribution is conducted in a secure manner, prior to any group being established. These keys can be established using various key establishment methods in ISO/IEC 8732 (ISO, 1988), ISO/IEC 11770- 1 (ISO, 1996a) and ISO/IEC 11770-2 (ISO, 1996b). There are several accepted methods that can be used to distribute keys to the communicating entities, including via physical (manual) delivery techniques, using other key to encrypt keys (key encrypting keys), or using a trusted third party.
- Key storage is managed in environments equipped with secure technology. For example, tamper-resistant hardware can be used to increase the level of security of the stored keys.
- Key installation is performed securely by all key managers (MKM and LKMs). We assume that a MKM is responsible for key installation at the domain level, and an LKM is responsible for key installation at the area level.
- Key revocation is conducted in a secure and proper manner by all key managers in a domain. We assume that a MKM governs any process to revoke keys at the domain level, and likewise an LKM at the area level. (f) Key disposal is handled in a secure and proper manner by all key managers such that no other information can be used to recover the disposed keys. We assume that MKMs and LKMs manage key disposal processes.

Secure Channels

We use the term *secure channel* to mean that communication between group entities (key managers and group members) within the KGMF is protected by careful application of symmetric keys.

This is achieved as follows:

- Key managers (MKM and LKMs) at the domain level secure the communications between them by using either a common key such as *domain key* for protecting communications between all key managers, or *Domain-Area* keys for secure communications between the MKM and each LKM separately.
- Local key managers and group members in the same area secure communications either by using a common *area key* for protecting communications between the LKM and all group members (residing within that area), *Area-Member* keys between the LKM and a group member separately, or *session mobility* keys between an LKM and a mobile member. Secure channels are created when group entities (MKM, LKMs and group members) use these keys in the course of group communication.

Group Membership Policy

In our proposal, while dynamic group membership is assumed throughout the framework design, the option for static group membership is also made available.

Design Approach

The assignment of key manager(s) can be *centralized*, *distributed*, or *hybrid*. Our proposal adopts the hybrid approach in the assignment of key managers, and is based on a distributed hierarchy of trusted entities (MKM and LKMs) for key management.

CONCLUSIONS

Secure group communication is an increasingly popular research area having received much attention in recent years. Group Key Management Framework applications in WSN demand for the security services to achieve the secure group communication. A common method is to encrypt messages with a group key so that entities outside the group cannot decode them. Therefore, key management is a basic structural development for secure group communication systems. This paper introduces a Group Key Management Framework method for WSN with multiple groups. We have used a group key based approach for transmission of information within members.

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.*