ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 11, November 2013

Survey Of Key Management Schemes For Secure Group Communication With Heterogeneous Environment In Wireless Sensors Networks

Priyanka Manhas[1] (Student)
Department of Computer Science & Engineering.
Chandigarh University (Gharuan, Mohali) India

Parminder Kaur[2](Asstt. Prof.)
Department of Computer Science & Engineering.
Chandigarh University (Gharuan, Mohali) India

Abstract- **A group communication benefits from IP multicast to achieve to scalable exchange of messages. IP multicast itself does not provide any mechanism for preventing non group members to have access to the group communication. Although encryption can be used to protect messages exchanged among group members. There are different approaches to group key management these approaches can we divided into three main classes: *Centralized group key management protocols, decentralized architectures and distributed key management protocols.* There is a challenge of effectively controlling access to the transmitted data. Key management scheme classified namely for *homogeneous* and *heterogeneous* environment. In this paper, we propose deployment conscious security framework with performance of proposed key management schemes is evaluated across relevant matrices. The area of group key management is surveyed and proposed with the help of his characteristics. Through our work we able to conclude that hybrid of asymmetric and symmetric key best suits on heterogeneous environment where key management in heterogeneous wireless sensor network nodes comprise of H- sensors and L-sensors.**

Keywords- **Asymmetric Key, Group Key Distributions, Heterogeneous, Key Management, Multicast Security, Wireless Sensor Network.**

I INTRODUCTION

WIRELESS sensor network (WSN) consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling *control* of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. IP multicast does not provide mechanisms to limit the access to the data being transmitted to authorized The security challenge for multicast is in providing an effective method for controlling access to the group and its information that is as efficient as the underlying multicast. A primary method of limiting access to information is through encryption and group members selective distribution of the keys used to encrypt group information. An encryption algorithm takes input data (e.g., a group message) and performs some transformations on it using a *cryptographic key*. This process generates a ciphered text. There is no easy way to recover the original message from the ciphered text other than by knowing the right key [Schneider 1996]. Applying such a technique, one can run secure multicast sessions. The messages are protected by encryption using the chosen key, which in the context of group communication is called the *group key*. Only those who know the group key are able to recover the original message. Wireless sensor network consist of some H-sensors and L-sensors that H-sensor apply as the cluster head because of their power in processing and memory and L-sensors are node's cluster members. Communication between nodes must be secure so H-sensors are reasonable for authentication and security. The number of H-sensor are not too much But they are more powerful that L-sensors so using H-sensors in key management and reduce money and consume memory. First H-sensors pre-distribute with keys and H-sensors pre-load L-sensor with key similar BS works in front of H-sensors. In this scheme key pre-distributed scheme based on random key predistributed for Heterogeneous sensor network.

The survey will unfold as follows: in section 2, we give guidelines for WSN design and deployment with key management role. The main contribution of this paper is described in section 3 and 4, where we present and analyze secure group key management protocols and also discus key management schemes based on heterogeneous frame. In section 5, presents analysis of wireless sensor networks nodes based on H-Sensor and L-Sensors and, finally section 6 will state the conclusion of this study.

II GUIDELINES FOR WSN AND KEY MANAGEMENT ROLE.

This application note is geared towards providing guidelines for building a wireless sensor network using MoteWorks tools based on application specific requirements. The guidelines include selection criteria for network topology, battery lifetime estimation, understanding effects on network performance by different network design choices:

Selection of Network Topology

There are three main network topologies in which a network can be organized:

1) *Star:* A single base station node directly communicates with multiple low power edge nodes
2) *Hybrid-star network*: A powered backbone of nodes form the routing infrastructure and edge nodes simply connect to any node in the backbone for communicating with the base station
3) *Mesh:* Each node communicates with its one hop neighbors to form multihop paths for data routing. The network is self-forming, self-healing due to availability of multiple alternate routes and provides maximum flexibility for route selection.

The following factors affect the design decision for selecting the appropriate network topology for a given customer application.

1) *Scale of the network*: The star topology will suffice for a small scale network where sensor nodes within the radio range of the base station directly communicate with it. The number of nodes that such a base station can support depends on the bandwidth supported by the type of node used as a base station. A PC as a base station can support more number of connections compared to a mote or Stargate node. For example in a Bluetooth network there is a master node controlling a limited number of edge/slave nodes within proximity. In order to scale the network over a larger geographical coverage, a hybrid-star or mesh topology is more desirable. In a hybrid star topology several wide spread nodes may connect to the powered backbone of nodes or in a true mesh network nodes spread over a large area may communicate using multiple hops.
2) *Availability of router nodes and battery lifetime*: If the user wants to organize the network in a hierarchical manner, where edge nodes perform simple data gathering tasks and router nodes perform communication and computation intensive tasks then a star or hybrid-star topology is best suited. The advantage of the hierarchical network organization is extended network lifetime for the battery operated sensor nodes at the cost of keeping line powered router nodes awake all the time. If the user does not distinguish between a sensor node and a router node, then all nodes are homogeneous in terms of their functionality and may form a low power mesh. In a mesh all nodes are battery powered and drain their energy faster compared to the battery powered edge nodes in a hybrid-star topology since they sense as well as route data.
3) *Physical separation among nodes*: The message reachability to the base station from a sensor node is constrained by its radio range. For a network deployment that requires sensor nodes to be separated by distances that are several times their radio range, intermediate router/gateway nodes are required to route messages to the base station. In such a deployment scenario, the star topology would have to be adapted to a hybrid star topology, where additional router may carry packets multihop or gateway nodes with longer radio range (for example a Stargate gateway with Wi-Fi radio for long range transmission) may be used. A mesh network will also allow a sparsely deployed network of nodes with large separations to exchange data through additional intermediate nodes deployed to form a well connected multihop network.
4) *Reliability*: Both hybrid-star and mesh network offer end-to-end message reliability. Hybrid-star networks are reliable since they use a powered backbone for routing where router nodes are always awake. With sufficient density of router nodes, one can assume that the backbone node would support the desired volume of network traffic and adequately serve all the battery powered edge nodes. Mesh networks are inherently fault tolerant since there are multiple alternate routes among nodes and a single point of failure does not exist. Therefore a true mesh is the most reliable network topology. The powered router backbone in hybrid-star may form a mesh too for enhanced end-to end message reliability at the router layer.

5) *Flexibility:* Mesh networks provide maximum flexibility since all nodes are identical in their functionality and can easily switch roles if there is a node failure or network congestion. Whereas in a hybrid star topology, placement of router nodes should be done strategically in order to provide a stable routing infrastructure with minimum nodes. Also there should be adequate redundancy at the router node level, so that edge nodes can access multiple parent router nodes for enhanced reliability. Since high power router nodes are expensive their network is sparse and failure of these nodes can significantly affect the network performance.

Key Management Role

Key management plays an important role enforcing access control on the group key (and consequently on the group communication). It supports the establishment and maintenance of key relationships between valid parties according to a security policy being enforced on the group.:

1) *Providing member identification and authentication*. Authentication is important in order to prevent an intruder from impersonating a legitimate group member. In addition, it is important to prevent attackers from impersonating key managers. Thus, authentication mechanisms must be used to allow an entity to verify whether another entity is really what it claims to be.
2) *Access control*. After a party has been identified, its join operation should be validated. Access control is performed in order to validate group members before giving them access to group communication1 (the group key, in particular).
3) *Generation, distribution and installation of key material*. It is necessary to change the key at regular intervals to safeguard its secrecy [Schneider 1996]. Additional care must be taken when choosing a new key to guarantee key independence. Each key must be completely independent from any previous used and future keys, otherwise compromised keys may reveal other keys.

Key secrecy can be extended to membership charges when group require for forward and backward secrecy. *Backward secrecy* is used to prevent a new member from decoding messages exchange before it joined the group if a new key distributed for the group when a new members joins, it is not able to decipher previous messages even if it has recorded earlier messages encrypted with old key.

Forward secrecy is used to prevent a leaving or expelled group members to continue accessing the group communication if the key is changed as soon as member leaves, that member will not able to decipher group messages encrypted with the new key.

III SECURE GROUP KEY MANAGEMENT PROTOCOLS:

Secure group key management protocols are explained on the basis of key management.
Key management is majorly divided into three categories: *Symmetric, asymmetric and hybrid.* WSN consist of numerous small, low cost, independent nodes, which have limited computing and energy resources. Secure and scalable WSN application requires efficient key distributions and key management mechanisms. A Group key management divided into three classes: *Centralized group key management protocols, Decentralized Architectures and distributed key management protocols.* Group communication has several advantages: *efficiency achieved, saving bandwidth, Scalable and no authentication or access control enforced.*
The literature presents us with several different approaches to group key management.

We can divide them into three main classes:

1) *Centralized group key management protocols*. A single entity is employed for controlling the whole group, hence a group key management protocol seeks to minimize storage requirements, computational power on both client and server sides, and bandwidth utilization.
2) *Decentralized architectures*. The management of a large group is divided among subgroup managers, trying to minimize the problem of concentrating the work in a single place.
3) *Distributed key management protocols*. There is no explicit KDC, and the members themselves do the key generation. All members can perform access control and the generation of the key can be either contributory, meaning that all members contribute some information to generate the group key, or done by one of the members.

Furthermore, the group may require that membership changes cause the group key to be refreshed. Changing the group key prevents a new member from decoding messages exchanged before it joined the group. If a new key is distributed to the group when a new member joins, the new member cannot decipher previous messages even if it has recorded earlier messages encrypted with the old key. Additionally, changing the group key prevents a leaving or expelled group member from accessing the group communication (if it keeps receiving the messages). If the key is changed as soon as a member leaves, that member will not be able to decipher group messages encrypted with the new key.

However, distributing the group key to valid members is a complex problem. Although rekeying a group before the join of a new member is trivial (send the new group key to the old group members encrypted with the old group key), rekeying the group after a member leaves is far more complicated. The old key cannot be used to distribute a new one, because the leaving member knows the old key. Therefore, a group key distributor must provide another scalable mechanism to rekey the group. Resiliency and connectivity are two important factors in proposed scheme. The scheme comprise of four stages: *Key Predistribution and Localization, Seeds Assignments, Deriving New Keys and Shared Discovery Keys.* The comparison of these four stages is as follows:

Predistribution Phase	**Computing Numbers of Seeds needed for Each cluster**	**Computing new keys by seed**	**Shared key Discovery**
In first stage, key pool is generated and phase keys are applied but derived keys are not used. Each nodes stores one base key of K base keys randomly.	Minimum Numbers of seed is equal to Numbers of cluster because, each cluster has one key. Each h sensor is the cluster head at each cluster head sends its location in operational environment of network grid.	Cluster head receives seeds from BS and compute new keys and send it to nodes cluster and this message encrypt by keys of bad cluster. Some seed are sent to cluster node by their cluster head. Node generate new key by using distance.	Each node transmit a message that encrypt by key cluster, this message contains its keys as a result neighbor node find shared key. If multiple shared key exist, one of them is selected randomly, but id the shared key does not exist, each node sends request message that contains its ID.

IV KEY MANAGEMENT SCHEMES BASED ON HETEROGENEOUS FRAME:

Key management schemes in Heterogeneous wireless sensor network comprising of wireless sensor nodes that are divided into H Sensors and L Sensors. H-sensor nodes are more powerful than L-sensor nodes in term of processing and memory. Because of that H-sensors are considered as the cluster head and L-sensor as the cluster member. H-sensor is responsible for the security of this communication. Each node can communicate with neighbor nodes. Problems of the network are security and battery lifetime for each node.

Communication between two L-sensors in one cluster or two different clusters is possible. that the robustness of a security framework relies upon the strength of its key management schemes. Two architectures are available for wireless networks, distributed flat architecture and hierarchical architecture. It is clear that in many sensing applications, connectivity between all Sensor Nodes (*SNs*) is not required but some applications require explicit connectivity between every pair of nodes. Mostly wireless SNs merely observe and transmit data to those nodes with better routing and processing capabilities, and do not share data among themselves. Therefore, the hierarchical heterogeneous network model has more operational advantages than the flat homogeneous model for WSNs with their inherent limitations on power and processing capabilities [11][12][13][8] and [12] *SNs* of heterogeneous WSN are divided into two categories namely H-Sensors and L-Sensors. H-Sensors are small number of *SNs* possessing higher memory, transmission range, multiple transmission ranges, processing power and battery life. Our network model has four different kinds of wireless devices on the basis of functionality; sink
node/base station (*BS*), cluster head node (*CH*), Anchor Nodes (*AN*) and sensor node (*SNs*).

1) *Sensor node* **(** *SNs* **):** Sensor nodes are new generation LSensors which are inexpensive, limited-capability, generic wireless devices. Each *SNs* has limited battery power, memory size, data processing capability and short radio transmission range. *SNs* communicate with its*CH* , *cluster SNs* and *SINK* . These are assumed to be capable enough to support the PKI. We propose to store two different encryption algorithms i.e. one for asymmetric key cryptography and one for symmetric key cryptography. We propose to use Elliptical Key Cryptography (ECC) for asymmetric key and Advance Encryption standard (AES) for symmetric key.
2) *Cluster head node* (*CH*): Cluster head nodes are a kind of H-Sensors, have considerably more resources than the *SNs* . Equipped with high power batteries, large memory storages, powerful antenna and data processing capacities(not exploited in this paper). *CHs* can execute relatively complicated numerical operations and have much longer radio transmission range than *SNs* .*CHs* can communicate with each other directly and relay data between its cluster members and the *SINK* . *SNs* which need to communicate with neighbors in neighboring cluster will relay its data through *CHs* . *CHs* are responsible for dividing *SNs* into clusters of uniform size.
3) *Anchor Nodes* **(** *ANs* **):** Anchor Nodes are a special kind of H-Sensors which have multiple power level for transmission. Thus *ANs* have capability to transmit in multiple ranges which can be changed at requirement. *ANs* are placed at triangular/Hexagonal points to realize a new grouping approach.

V ANALYSIS OF WIRELESS SENSOR NETWORKS NODES BASED ON H-SENSOR AND L-SENSORS

Wireless sensor networks' nodes are divided to H-sensors and L-sensors. H-sensor nodes are more powerful than L-sensor nodes in term of processing and memory. H-sensor is responsible for the security of this communication. Each node can communicate with neighbor nodes. Communication between nodes must be secure so H-sensors are reasonable for authentication and security. First H-sensors pre-distribute with keys and H-sensors pre-load L-sensor with key similar BS works in front of H-sensors. *the keys pre-loaded in nodes with cluster head and is not need to preload with BS also derived keys.* Communication between two L-sensors in one cluster or two different clusters is possible. Base station (BS) is assumed to be secures and resources such as energy process power and memory are not limited. H-sensors are more powerful in terms of memory and processing than L-sensors. H-sensors are connected to BS directly.

There are some assumption as follows :

1) Assume that H-sensors and L-sensors are distributed randomly in operational environment.
2) H-sensors are clusters head and L-sensors are as the cluster members.
3) Suppose that networks are secured in distribution phase and only capture node along communication.
4) Location of L-sensors and H-sensors are static.
5) Range transfer of H-sensors and L-sensors are static.
6) Range conduction of H-sensors are high.
7) Number of sensor nodes in a cluster is assumed tobe not determined.
8) Each H-sensor have GPS and report locations.

The amount of H-sensors is not too much and number of seeds is enough, so seeds meet key management requirements, therefore a little amount of seeds will belonged to H-sensors (Sb).

VI CONCLUSION

In this article, we presented a survey in the secure group communication area, particularly regarding the secure distribution and refreshment of keying material. We reviewed several proposals, placing them into three main classes: group key management protocols, which try to minimize the requirements of group members; decentralized architectures, which divide large group in smaller subgroups in order to make the management more scalable; and finally, the distributed key management protocols, which gives all members the same responsibilities. Primarily, the usage of security mechanism for secure group communication should be made transparent to the user and it should also work well with other protocols. we propose a key management scheme for heterogeneous sensor networks based on random key predistribution. In our scheme, instead of storing all the assigned keys in a sensor node, we store a small number of generation keys. Adversary or malicious nodes are precluded to join the cluster as each L-sensor is authenticated by CH using L-sensor's authentication key. The keys preloaded nodes with cluster head and is not need to preload with Base Station also derived keys. The schemes evaluated by MATLAB. We also discus four stages of group key communication for secure wireless sensor network in tabular form.

REFERENCES

[1] Banihashemian, Saber and Ghaemi Bafghi, Abbas. A new key management scheme in heterogeneous wireless sensor networks. Mashhad: Ferdowsi University of Mashhad (FUM), 2011.

[2] An effective key management scheme for heterogeous sensor networks, Ad Hoc Networks. Du, X., et al. 2007, Vols. 24-34.

[3] M. Eltoweissy, H. Heydari, L. Morales and H. Sudborough, "Combinatorial Optimization of Group Key Management", J Network and System Management, vol. 1, no. 12, **(2004)**.

[4] BALLARDIE, A. 1996. *Scalable Multicast Key Distribution*. RFC 1949.

[5] BALLARDIE, A. AND CROWCROFT, J. 1995. Multicast specific security threats and counter-measures. In *Proceedings of the Symposium on Network and Distributed System Security*. (San Diego, Calif., Feb.).

[6] BECKER, C. AND WILLE, U. 1998. Communication complexity of group key distribution. In *Proceedings of the 5th ACM Conference on Computer and Communications Security*. (San Francisco, Calif., Nov.). ACM, New York.

[7] BOYD, C. 1997. On key agreement and conference key agreement. In *Proceedings of the Information Security and Privacy: Australasian Conference*. Lecture Notes in Computer Science, vol. 1270. Springer-Verlag, New York, 294– 302.

[8] Bulusu V, Durresi A, Paruchuri V, Durresi M, Jain R (2006) Key distribution in mobile heterogeneous sensor networks. In: Global telecommunications conference, 2006. GLOBECOM '06. IEEE, New York, pp 1–5. ISBN 1-4244-0356-1

[9] Chan H, Perrig A (2005) Pike: peer intermediaries for key establishment in sensor networks. In: INFOCOM 2005. 24th annual joint conference of the IEEE computer and communications societies, pp 524–535. ISBN 0-7803-8968-9

[10] Du X, Lin F (2005) Maintaining differentiated coverage in heterogeneous sensor networks. EURASIP J Wirel Commun Netw (4):565–572

[11] Du X, Xiao Y (2006) Energy efficient chessboard clustering and routing in heterogeneous sensor network. Int J Wirel Mobile Comput 1(2):121–130

[12] Du X, Xiao Y, Guizani M, Chen H-H (2007) An effective key management scheme for heterogeneous sensor networks. Ad Hoc Netw 5(1):24–34

[13] Duarte-Melo EJ, Liu M (2002) Analysis of energy consumption and lifetime of heterogeneous wireless sensor networks. In: Proceedings of IEEE GLOBECOM, 2002

[14] Lazos L, Poovendran R (2006) Stochastic coverage in heterogeneous sensor networks. ACM Trans Sensor Netw (TOSN) 2(3):325–358

[15] Firdous K., Sajid H., Laurence T. Y., Ashraf M. 2008. Scalable and efficient key management for heterogeneous sensor network. *Journal of Supercomput* . 45(2008), 44–65.