Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

# A key distribution scheme for secure communication in acoustic sensor networks

Md. Abdul Hamid [a], M. Abdullah-Al-Wadud [b], Mohammad Mehedi Hassan [b,*], Ahmad Almogren [b], Atif Alamri [b], Abu Raihan M. Kamal [c], Md. Mamun-Or-Rashid [d]

[a] Department of Computer Science, Faculty of Science & Information Technology, American International University-Bangladesh, Dhaka, Bangladesh
[b] Research Chair of Pervasive and Mobile Computing, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[c] Department of Computer Science & Engineering, Islamic University of Technology, Gazipur, Bangladesh
[d] Department of Computer Science & Engineering, University of Dhaka, Dhaka, 1000, Bangladesh

## HIGHLIGHTS

- A new deterministic key distribution mechanism for acoustic sensor networks.
- The construction methodology uses the properties of regular Hexagon.
- The configurations have a compact and efficient algebraic description.

## ARTICLE INFO

*Article history:*
Received 20 January 2017
Received in revised form 20 June 2017
Accepted 10 July 2017
Available online xxxx

*Keywords:*
Acoustic sensor networks (ASNs)
Key distribution
Hexagon
Communication security
Wireless network

## ABSTRACT

Cryptographic key distribution is always a major problem in large scale wireless communications such as Acoustic Sensor Networks (ASNs) based on wireless sensors in an Internet of Things (IoT) environment. Because of the resource constraints of the nodes in such networks, the traditional cryptographic primitives are not suitable solutions. Our endeavor in this paper is to develop a new deterministic key distribution mechanism for such networks. In particular, we bring in a novel construction methodology from two-dimensional geometry by exploiting the properties of regular Hexagon. One advantage of using the proposed approach, as opposed to randomized distribution techniques, is that, the configurations have a compact and efficient algebraic description. This yields nice algorithm for shared-key discovery, in which very little information (or no information at all) needs to be broadcasted. Furthermore, it is shown that the security strength of the proposed approach outperforms well-known deterministic techniques in terms of resilience. Furthermore, the distribution technique ensures 100% connectivity (i.e., the probability that two nodes share a key is 1) and average key-path length is 1.



## 1. Introduction

Acoustic sensor networks (ASNs) are usually deployed to monitor vast environment underwater and underground with the help of a large number of sensors. With the penetration of the Internet of Things (IoT) paradigm, the scope ASN is growing so fast to be integrated in different smart monitoring systems such as monitoring and surveillance, underwater and underground exploration, disaster prevention and recovery, and many other applications. The scope is growing to collect data from many different systems built on wireless sensor networks composed of low power and resource constraint sensors as a huge source of data. Such sensor networks are mainly responsible for collecting different data about devices and environment under consideration, and sending the data to sinks in a single or multi-hop fashion, necessitating a large number of nodes to communicate with each other to send the collected data to sink. Securing such communication is hence very important in order to maintain privacy and other security issues associated with data collection services [1–5]. However, due to the resource constraints of sensor networks, traditional cryptographic primitives are not suitable solutions. More specifically cryptographic key distribution is always a major problem in such an environment. Basically, a key distribution scheme has 3 phases: (i) key distribution, (ii) shared key discovery and (iii) path-key establishment. During these phases, secret keys are generated and placed in nodes, and each node searches the area in

* Corresponding author.
*E-mail addresses:* hamid@aiub.edu (M.A. Hamid), mwadud@ksu.edu.sa (M. Abdullah-Al-Wadud), mmhassan@ksu.edu.sa (M.M. Hassan), ahalmogren@ksu.edu.sa (A. Almogren), atif@ksu.edu.sa (A. Alamri), raihan.kamal@iut-dhaka.edu (A.R.M. Kamal), mamun@cse.univdhaka.edu (M. Mamun-Or-Rashid).

http://dx.doi.org/10.1016/j.future.2017.07.025
0167-739X/

its communication range to find another node to communicate. A secure link is established when two nodes discover one or more common keys, and communication is done on that link between those two nodes. Afterwards, paths are established connecting these links to create a connected graph. The result is a wireless communication network functioning in its own way according to the key distribution scheme used in creation.

Networks, be it wired or wireless, are exposed to the same basic threats: messages can be intercepted, modified, delayed, replayed, or new messages can be inserted. A network and provided resources could be accessed without authorization, and they could be made unavailable by denial of service attacks. In general, security threat or attack attempts to gain unauthorized access to a service, resource or information, or to compromise integrity, availability, or confidentiality. Information security manifests itself in many ways according to the situation and requirements. Regardless of the degree of involvement, all parties concerned with a transaction must have confidence that certain objectives associated with information security have been met. Different security schemes are used to achieve the communication security in the networks, and are designed to serve these paramount objectives. Cryptographic key distribution is a vital part to achieve such objectives [6–8].

An efficient key pre-distribution scheme should ensure high probability of secure connections, good expansibility to facilitate the increase of the number of nodes in a network, low cost and strong resistibility against being captured. In general, key distribution schemes can be classified into four kinds: probabilistic schemes [9–11], deterministic schemes [12–15], hybrid schemes [16,17] and location aware or group-based schemes [18–21]. Traditional key exchange and key distribution protocols based on infrastructures using trusted third parties are impractical for distributed sensor networks. This is because of the unknown network topology prior to deployment, communication range limitations, intermittent sensor-node operation, and network dynamics. Therefore, the practical solution for the distribution of keys to sensor nodes whose physical topology is unknown prior to deployment would have to rely on key distribution. Keys are to be installed in sensor nodes to accommodate secure connectivity between nodes. However, traditional key pre-distribution offers two inadequate solutions: either a single mission key or a set of separate keys, each being pair-wise and privately shared with another node, must be installed in every sensor node. However, single mission key alternative is insufficient because the imprisonment of any sensor node may compromise the entire sensor network since selective key revocation is impossible upon sensor imprisonment detection. In contrast, the pair-wise shared key(s) between every two sensor nodes avoids network wide compromise upon node imprisonment since selective key revocation becomes possible. However, this solution requires pre-distribution and storage of large number of keys in each sensor node, which is unrealistic when the number of nodes are very large, for both intrinsic and technological reasons. Nevertheless, symmetric key distribution approach is used in past research, but with a focus on group and broadcast communication. For group communication, different researches [13,22] try to accommodate a set of users while being secure against collusion between some of them. Pre-distribution is used to alleviate the cost of communication between group members and to setup a common secret key. But, memory constraints are not placed on group members. Some other research on broadcast encryption [23] focuses on key distribution to support broadcast communication between slave nodes and a master node an impractical approach for network with large number of nodes.

In this paper we propose a key distribution mechanism that addresses the above mentioned problems, i.e., (i) each node needs to store few number of keys, (ii) any two communicating nodes shares common key(s) with 100% probability. Finding common key(s) is easy since the well-defined mathematical solutions are provided by our protocol, and it alleviates the problem of path key establishment.

We present a deterministic key distribution mechanism based on the geometric properties of regular hexagons. Though a lot of efforts [24–29] have been dedicated to develop protocols for wireless networks based on the geometric properties of hexagon, most of the existing protocols in the literature focus on connectivity, placement of the nodes, routing strategy, or capacity in wireless networks. Security considerations, especially in this domain, remain unfocused, except the one in [30] that focuses on the hexagon based key distribution but necessitates the overhead of some broadcast messages to establish pair-wise communication keys.

We develop a novel construction methodology from two-dimensional geometry by exploiting the properties of regular hexagons. The proposed method lets each node have a set of keys of which it shares a distinct subset with every other node. Also, this yields nice algorithms for shared-key discovery, in which very little information (or no information at all) needs to be broadcasted. We discuss the performance in terms of security and storage requirement. We present security analysis in terms of the minimum number of colluding nodes needed to compromise a pair of nodes' conversation key. Also, we estimate the memory costs and other parameters. It is shown that the security strength of the proposed approach outperforms well-known deterministic techniques in terms of resilience. Finally, we discuss possible extensions to improve performance and/or security, and potential applications.

The rest of the paper is organized as follows. In Section 2, we discuss some works related to the proposal in this paper. We present the proposed hexagon based key distribution mechanism in Section 3 followed by the performance analysis presented in Section 4. Finally, in Section 5, we conclude our paper.

## 2. Related works

Different symmetric-key distribution schemes can be classified into two categories, namely probabilistic and deterministic schemes. The probabilistic schemes [31–35] rely on probabilistic key sharing among the nodes of a random graph and use a simple shared-key discovery protocol for key distribution, revocation and node re-keying. Eschenauer et al. in [31] proposed a random key pre-distribution scheme where tens to hundreds of keys are uploaded to sensors before the deployment. In their solution, a large key-pool, $P$, is generated initially. For each sensor, $k$ keys are randomly drawn from the key-pool $P$ without replacement. These $k$ keys and their identities form a key-chain which is loaded to the sensor node. Two neighboring nodes compare the list of key identities in their key-chains. Eschenauer et al. also proposed to employ a Merkle Puzzle [33], similar approach to secure the key identities, which requires too much processing and storage for a resource limited sensor node. After exchanging key identities, common keys are used to secure the link in between two sensor nodes. It may be the case that some of the neighboring nodes may not be able to find a key in common. These nodes can communicate securely through other nodes, through other secured links.

Chan et al. [32] proposed a modification to the basic scheme of Eschenauer et al. They increase amount of key overlap required for key-setup in order to increase the security of communication between two neighboring nodes. Their proposal requires larger key-chains and smaller key-pools than the original proposal of Eschenauer et al. In [34], common keys in the key-chains are used to establish multiple logical paths over which a costly threshold key sharing scheme is used to agree on a new secret.

The probabilistic schemes have no computational overhead, but the communication overhead is proportional to the total number

Please cite this article in press as: M.A. Hamid, et al., A key distribution scheme for secure communication in acoustic sensor networks, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.07.025.