The ISC Int'l Journal of Information Security

July 2016, Volume 8, Number 2 (pp. 117–132)

http://www.isecure-journal.org

A Novel Key Management Scheme for Heterogeneous Sensor Networks Based on the Position of Nodes☆

Taha Yasin Rezapour [1,2], Reza Ebrahimi Atani [1,*], and Meer Soheil Abolghasemi [1]

[1] *Department of Computer Engineering, University of Guilan, Rasht, Iran*

[2] *Department of Information Technology, Ports and Maritime Organization, Tehran, Iran*

ARTICLE INFO.

Article history:
Received: 23 April 2014
First Revised: 13 May 2015
Last Revised: 29 May 2016
Accepted: 2 July 2016
Published Online: 27 July 2016

Keywords:
WSN; Position Based Cryptography; Key Management; Heterogeneous Sensor Networks.

ABSTRACT

Wireless sensor networks (WSNs) have many applications in the areas of commercial, military and environmental requirements. Regarding the deployment of low cost sensor nodes with restricted energy resources, these networks face a lot of security challenges. A basic approach for preparing a secure wireless communication in WSNs, is to propose an efficient cryptographic key management protocol between sensor nodes to achieve maximum security with minimum cost. The main motivation of this paper is to apply the position of the sensor nodes as part of their identity for key management in heterogeneous sensor networks. In the proposed scheme, the position of sensor nodes is considered as a part of their identity and it is used for authentication and dedicating key to all network links. Comparing the proposed technique with other schemes shows that it has a higher level of scalability, security, and reliability with less memory complexity.

1 Introduction

Recent progress in micro-electromechanical systems technology, wireless communications and digital electronics has provided the possibility of designing and manufacturing sensors with low power consumption, small size, reasonable price and various applications. These tiny sensors can perform activities such as receiving various environmental data based on the type of sensor, processing and sending the information. This was a good motivation to the idea of creating and developing wireless sensor networks (WSNs). These networks consist of a large number of small nodes, where each node comprises a number of sensors and actors. The main purpose of the deployment of WSN is serving as a mediator in order to provide real-world physical information such as temperature, pressure, light, sound, radiation, mobility and more [1, 2]. Sensors exchange information received from their surrounding environment with each other to create an overview of the area under their control. Access to the information for users outside of the network is possible by using the gateway communication. Rapid deployment, self-organization and fault tolerance capability of these networks has led to an increase in their application. In addition, WSNs have high node-density, availability and low cost that makes their development and maintenance easily possible.

Due to the growing use of new technologies in various fields, many applications can be identified for wireless sensor networks. These applications can be classified into two categories: "monitoring" and "tracking". Monitoring applications are such as monitoring

☆ This article is an extended version of an ISCISC'10 paper.

* Corresponding author.

Email addresses: rezapour@anzaliport.ir (T.Y. Rezapour), rebrahimi@guilan.ac.ir(R. Ebrahimi Atani), soheil@guilan.ac.ir (M.S. Abolghasemi)

ISSN: 2008-2045

the internal/external environment, monitoring assets, factories, buildings and etc. Tracking applications include tracking objects, animals, people and vehicles [3, 24].

According to the characteristics of WSNs, like other types of networks; they are always exposed to various attacks by the attackers to penetrate and disrupt the system. The adversaries manipulate data (listening, modifying, implementing, removing and noise). Nature of wireless communication, lack of infrastructure and an uncontrolled environment increases the capabilities of the adversaries in sensor networks. Attackers having laptops, batteries and powerful antennas are capable of being mobile and moving around or into the sensor networks. Wireless communication helps adversaries to perform different types of attacks. For example, Denial of Service attack (DoS) is an explicit attempt to make services or resources unavailable to the users. A DoS attack can reduce or cut any networking capabilities to perform tasks that would be expected. Hardware, failures, software bugs, resource draining, overflows or any activity which involves factors such as these will lead to DoS attack. "Sinkhole" attack is another example that is known as the "Black hole" attack. It aims to capture all the traffic from a particular area which provides a black hole in the network. This attack typically provides a routing protocol by creating a way to capture other nodes. Another attack is the "Wormhole" attack. In this attack the adversary receives the packets from a specific place and transfers them to another location on the network by tunneling through a link with low latency, which is controlled by the adversary. The wormhole attack is a serious threat to sensor networks, which can disrupt the routing protocols. Without having an appropriate mechanism to deal with this attack, most existing routing protocols are not able to create a compatible path between pairs of nodes. If the adversary passes the packets from one point to another by tunneling, it may seem that a reliable service is provided to transmit the packets. Wormhole attacks do not need to compromise the authorized nodes, they can also implemented by external identities and internal identities. This type of attack will be executed even during the initial setup of the network in order to convince the neighbor nodes [1, 4].

Security is a very important component for the achievement of actual functionality in sensor networks. Thus, security mechanisms must always be considered in their network architecture design. It is not easy to apply traditional encryption techniques directly in the design of sensor networks, providing key management including key production, distribution and revocation as a basic approach in the network security is a topic that recently has been very significant to researchers. Therefore, various cryptographic key management schemes are proposed for this type of Adhoc networks. Most of these projects were proposed for sensor networks with a homogeneous structure. However, because of some limitations such as performance and scalability of homogeneous sensor networks, researchers started to consider these networks with heterogeneous structure [19, 20]. Recently, a number of key management schemes for heterogeneous sensor networks are presented. In [21] a survey on secure localization and location verification in wireless sensor networks is presented. Actually the locations of sensor nodes are very important in many WSNs. When WSNs are deployed in hostile environments, two issues about sensors' locations need to be considered. First, attackers may attack the localization process to make estimated locations incorrect. Second, since sensor nodes may be compromised, the base station (BS) may not trust the locations reported by sensor nodes. So far several location based security models for WSN key management are presented, but after presentation of state of the art position based cryptography [16, 25] and its differences with location based cryptography some new attributes were presented to the community which could easily solve location based protocols [18]. Therefore, with respect to this important issue, in this paper a new scheme for key management in wireless sensor networks with heterogeneous structure is presented. This scheme is based on the position of the sensor nodes. In fact, using the position of the sensor nodes as part of their identity for authenticating the new scheme for key management in the network and sensor nodes is presented. The main contribution of this works is to design and analyze the security of a position based key management schemes for homogeneous sensor networks. To the best of knowledge of the authors this is one of the few position based key management models for WSNs. The required key storage space, especially primary keys on most presented schemes is an important challenge for the researchers (due to the use of the key pool pre-distribution mechanism in many schemes and even a large number of required keys to preload the other plans that do not use the key pool). In this technique using position as primary information for session key generation, a significant reduction of the primary key for the pre-distribution of the sensors is achieved (one key for each cluster head). This scheme supports scalability (adding new SN or remove SN with no battery lifetime) and mobility for SNs in networks domain. This model can be implemented for applications such as smart control of containers in the ports and decks in the industry of ports and maritime given the importance of the position of the containers [22].

The rest of this paper is organized as follows, in

Section 2 the related work is reviewed. In Section 3 in addition to description of position based cryptography and position based key exchange; the required assumptions to present the new scheme are discussed. In Section 4 key management scheme based on position for heterogeneous sensor networks is presented in details. In Section 5 security evaluation of the proposed technique is presented and finally the paper is concluded in Section 6.

2 Related Work

In this section a number of provided related work are considered.

"Escheauer" and "Gligor" [5] proposed the first random key pre-distribution scheme for bootstrap keys in sensor networks. Each node with a key ring contains randomly selected from a pool of random keys, which is selected from a pool of pre-loaded keys. Establishing a secure link between two nodes that are within a radius of each other's wireless communications depends on the probability of sharing at least one key in their key rings. In the key pre-distribution phase for each node a number of keys from a pool of keys with given size were randomly selected and stored in the memory of each node. The keys for each node are called the node's key ring. The nodes then run the key discovery phase to identify keys that are shared with their neighbors (if neighbors exist). A key is shared between the two neighbors for communication. The key sharing graph is assumed as a random graph with no prior knowledge of nodes which will be neighbors after arrangement of the network. Sensor nodes vertices and edges are secured connections by the shared key among the neighbors. If the key sharing graph is connected, in the phase of path key establishment, each pair of nodes that do not have a common key must be able to create a path key through the secure pairwise connections.

"DU" *et al.* [6] presented a key management method based on modular arithmetic. In this scheme every membered sensor node only needs to store one key seed. This seed is used for measuring the shared key with other nodes in similar clusters. Additionally sensor nodes in the network can instantly update their key seeds. The scheme is also capable to reduce time delay and energy consumption of key deployment in WSNs with large scale. There is an offline base station in this scheme that is used to preload key for every sensor node in the network. The network consists of a multitude of clusters. There is a cluster head in order to distribute key seeds for membered sensor nodes in every cluster. Cluster heads can directly communicated with their neighboring cluster heads. In this scheme ECDSA (Elliptic Curve Digital Signature Algorithm) is used to evaluate cluster head's identity. Pre-key distribution phase and self-running phase are done. The other feature of this scheme is the capability of session key establishment for intra cluster and inters cluster communications.

"Kausar" *et al.* [7] proposed a key management scheme based on random key pre-distribution in the heterogeneous sensor networks. In this scheme, the network consists of two types of sensors, high-end sensor (H sensor) and low-end sensor (L sensor). In addition, hierarchical structure is used for scalable solutions in the proposed scheme. H sensors act as cluster headers and L sensors as cluster members. In this key management method, a hash-chain based technique is used for generating keys. Instead of generating a large pool of random keys, a key pool is represented by a small number of generated keys. A hash function gives a key chain for the generated key and obvious key materials. These key chains collect a key pool. Each sensor node is randomly referred to a small number of selected keys. As a result, using generated keys, the scheme improves the storage requirement properly. Since the dynamic topology of sensor networks is invitable, it should be possible to add or remove nodes. Considering this issue, the scheme allows the nodes to be added or removed. In case of adding a sensor node, the scheme can determine whether it is legal or the role is subversive. If the adversary compromises the sensors, all the keys will be updated periodically.

"Banihameshemian" and "Bafghi" [8] have presented scheme based on key distribution in a random way for heterogeneous sensor networks. In this scheme separate keys in different clusters and distance measurement of sensors from their cluster heads are used. Some of the base keys in sensors are pre-distributed and after network establishment new keys in belonging sensors to each cluster is established. Connectivity capability and flexibility are two thing that are considered in this scheme. It is assumed in this scheme that all H sensors are equipped with GPS that are aware of their positions. The main idea in this key management scheme is using cluster information and also node distance from head cluster. A new concept called level is used in this scheme in which nodes belonging to a particular level or based on their distance from cluster head. Every seed has its own distinct seed that is used to run new keys and is only applicable in that level and the neighboring level. Hence, network is categorized in sections which have different keys. This scheme consists of four stages including pre-key distribution, localization, seed devotion and shared key revelation. Key pool consists of main keys and driven keys. Loaded keys are hashed based keys with different seeds. Numbers of seeds for management necessities are satisfactory and large enough.

"Khan" *et al.* [9] proposed a scheme establishing

keys for heterogeneous sensor networks. The reference network model of a defined heterogeneous sensor network in this design consists of a base station, fixed nodes and mobile nodes. Base stations and fixed nodes are powerful devices, while mobile nodes are defined by very limited resources and are characterized by their position in a dynamic model that allows them to change their environment. Moreover, the number of mobile nodes is larger than the number of fixed nodes and only the fixed nodes need to be equipped with tamper-proof hardware requirements. In this scheme the base station can be associated only with fixed nodes and it acts as a trusted server. Fixed nodes act as cluster headers and are responsible for authentication management and key establishment operations for a group of mobile nodes. After the key pre-distribution operation in fixed and mobile nodes, clusters are formed. To access the network, each mobile node needs to establish its own authenticity for a selected cluster header. To do so, the mobile node sends an encrypted "append request" message with the public key of the network. The cluster header is able to deduce the mobile node authentication key using a one way authentication key generation function. For a secure communication between cluster header and the mobile node, a secret key is assigned to each mobile node, while its generating function is allocated to the fixed nodes before the arrangement. During the authentication phase, each cluster header receives the prime number of mobile node for the member nodes. The cluster headers use these mobile node's prime numbers and the generator of the secret key gives the first number using the prime generator. This prime is again combined with the prime numbers of mobile nodes and secret key generator to generate the next prime number. Then, the cluster header generates the required secret key using a one-way secret key generating function. For a secure connection among mobile nodes, a secret key is generated between them by the cluster header. For example, if a mobile node wants to establish a direct communication link with another mobile node, it sends its ID and the other node's ID to the cluster header. The cluster header generates a secret key for those two mobile nodes using the ID, prime number and one-way secret key generating function and sends it to both mobile nodes using a shared secret key with each of them. Cluster heads also notify the base station periodically about mobile member nodes to prevent repeated attacks on the network. In addition to this issue, in this scheme a procedure has been considered for the mobile nodes to leave a cluster and join another one based on the received signal strength of the fixed nodes that act as cluster headers.

"Alagheband" and "Aref" [10] presented a key management method based on elliptic curve cryptography and "signcryption" method. In this scheme,' which considers the network with a hierarchical structure, cluster headers are fixed while the sensor nodes are capable of mobility. Before initialization and cluster construction phase, a number of symmetric and asymmetric keys are embedded in all sensors. Due to the importance of communication between cluster headers and the base station and also cluster headers with each other, more stringent security policies are used to create links between them. In this scheme, sensor nodes registration is done using an algorithm based on "signcryption". It should be noted that the "signcryption" is a primitive public-key that simultaneously implements digital signature functions and encryption. The scheme also has a periodic authentication procedure to keep sensors secure against demodulation and also to support mobility of sensor nodes between the clusters, particularly in liquid environments.

"Huang" *et al.* [11] have presented a dynamic key management key scheme for wireless sensor networks in which a hash function in base station, cluster heads and sensor nodes are loaded. Then clusters and sensor nodes of chain key present themselves for authenticity. Cluster heads and sensor nodes, prepare paired keys to guarantee confidentiality of transmission. This scheme reduces the number of needed keys for sensor nodes and cluster heads and establishes an appropriate resistance against attacks such as guessing, reply attack, man in the middle, node capture and denial of service. Every cluster head establishes its own key chain that encrypts connections and messages with other sensors in the cluster. According to the applied hierarchical clustering, every cluster consists of several sensor nodes and one cluster head. H sensor is directly in communication with BS and transmits all received packets from L sensors to BS. The point that is considered in this method is that for L sensors to transmit messages to each other, they should perform it through a H sensor. In another words L sensors cannot directly communicate with each other. So compromising each L sensor does not have any effect on other L sensors. In Huang methods two scenarios are taking into account so as to receiving data from sensor nodes. In the first scenario data collecting from all normal sensor nodes is done through broadcasting a public message for all the cluster heads. In the second scenario, the base station sends a request to the cluster head for receiving data from a particular sensor node.

In [23] authors show that Zhang *et al.*'s scheme [26] does not achieve forward secrecy. They propose a new light weight location-based compromise-tolerant key management scheme for sensor networks, which can provide perfect forward secrecy. Their scheme can defend against various known types of attacks such as node compromise, key compromise impersonation

attack, identity replication attack, Sybil attack and wormhole attack. An additional important advantage of the scheme is that it does not need expensive pairing computations or map-to-point hash operations.

"Mala" *et al.* [12] have presented a hierarchical key management scheme based on random pre-key distribution. The motivation is to establish a safe tree instead of a completely connected graph. This scheme provides a safe tree that the sink is its root. It lets reduction of key storage overhead through restricting dependence on key sharing in parent child relationship. This scheme consists of two bases including pre-key distribution and parent child shared key revelation. In this scheme, in which the network scalability is considered, one heterogeneous sensor network that consist of strong base station and two types of sensor nodes are taken into account. The first group is small proportion of strong sensor nodes with a long radio radius that is called supper node which are indicated with Sn and the second group is a large number of simple nodes with short radio radius that are called normal node and is indicated with Nn. Because the type of sensor node influences the structure of tree, every node has an indicator in its sent message that shows the type of node (Nn or Sn). Contrary to a lot of other schemes in which a completely safe graph is constructed with a tree, in Mala's a safe path is made between each node and the sink. After preloading of every node with key chain, the sink broadcasts a tree request. Since the sink has stored the key pool, it is assured that all sensor nodes have at least shared one key with the sink. When a sensor node has received this request from the sink, the sink is chosen as parent and chooses one key from key chain as shared key with sink. Now this node joins the tree that its root is the sink.

"Du" *et al.* [13] With regard to weaknesses in terms of performance and scalability in homogeneous sensor networks, adopt a heterogeneous sensor network model. They proposed a novel routing-driven key management scheme, which only establishes shared keys for neighbor sensors that communicate with each other. This scheme utilize elliptic curve cryptography in the design of an efficient key management scheme for sensor nodes. The many to one traffic pattern dominates in most sensor networks, where all sensors send data to base station. Due to the many to one traffic pattern, a sensor node may only communicate with a small part of its neighbors, for example, neighbor sensors that are in the routes from itself to the base station. This means that a sensor node does not need shared keys with all neighbors. This scheme give a definition that considers the fact. A sensor node named v is a communication neighbor (c-neighbor) of sensor node u if v is in a route from u to the base station. Therefore, this scheme only needs to set up shared keys for each sensor and its c-neighbors, i.e., it does not need to set up shared keys for each pair of neighbor sensors.

"Ma" *et al.* [14] proposed a key management scheme for heterogeneous wireless sensor networks to improve the random key pre-distribution scheme using deployment knowledge of nodes and the prior area deployment information. This scheme divides the network sensing area into several sub regions; divides the key pool into several key pools, and divides nodes into several groups. Nodes in a certain group randomly select some keys from the corresponding key pools are deployed at the corresponding sub regions. This can improve the probability that neighboring nodes share common keys at a certain extent. Ma scheme consists of three phases: key pre-distribution, shared-key discovery, and path-key establishment. First phase is performed offline and before the deployment of sensor nodes. After deployment, network are divided into multiple clusters, after completion of clusters forming, each node needs to discover whether it shares any keys with its neighbors. After shared-key discovery phase, there is a direct shared-key graph in the cluster and between clusters. This graph consists of the nodes that establish the direct shared-key and their security link. The rest of nodes that cannot establish the direct shared-key could find the path key through this graph.

"Tian" *et al.* [15] proposed a key management scheme based on a keyed-hash chain approach which can support five types of communications. This scheme focus on a military heterogeneous sensor network scenario and supports the establishment and renewal of five types of keys in the network because single key cannot satisfy different communication requirements. All keys involved in this scheme are symmetric keys. Tian scheme's includes three stages: key pool generation, key ring assignment and common key discovery. Their scheme uses keyed-hash chain to reduce storage overhead. The essence of the suite of key management is a key pre-distribution scheme. An important point that must be considered in the review of this plan is that keyed hash function is the foundation of keyed hash chain. Keyed hash chain in this paper can be derived by generating a random key seed X and a generation key K; repeatedly applying the same keyed hash function to produce the hash chain. This scheme devote to establish five types of keys. These include (1) a master key shared between CHs and BS for sending aggregated data, (2) authentication keys shared by a CH and its cluster nodes for verifying messages shared by them, (3) pairwise keys shared by neighboring nodes within a cluster for intra-cluster node-to-node communication, (4) a cluster key for each cluster for broadcasting within a cluster, and (5) pairwise keys shared by cluster heads for inter-cluster

communications. In addition this scheme has a key revocation plan to prevent of node compromise and a procedure for add a new node for achieving scalability.

After evaluation of key management schemes in sensor networks we can classify them into two categories: In the first category, all keys in sensor nodes are predistributed and each node chooses a group of keys from key pool. Then in the boot strapping phase each node finds its neighboring shared keys. If a node cannot find a mutual key, then it will establish a shared key with the assistance of one or more of interface node. This category of schemes that are based on pre distributed key in an assumed way guarantee a high probability of keys sharing and the second category are schemes in which a number of key or seeds in sensor nodes are pre distributed. Session keys are also established due to a request. In most cases a number of nodes perform as head nodes or gateways for session keys establishment for both categories. Interface nodes are usually stronger than other membered nodes in following aspects: energy source, telecommunication range, data processing capability, storage space and tamper resistant. According to mentioned information in the classification above, assessed schemes in this section can be categories into parts that are illustrated in the Figure 1.

3 Definitions, Assumptions and Terminology

In this section, first we describe "Position-based cryptography" and its capability in key management applications and then assumptions in the proposed network model and the terminology used in the proposed scheme will be described afterwards.

3.1 Position-based Cryptography

In cryptography "identity" components are important to us. As a typical example we can mention the name and national ID card, so are scans of fingerprints or residential addresses, work addresses and so on. Data can be encrypted in a way that only the person who holds the private key can decrypt it (public key or private key). The question is whether or not it is possible we have other forms of "identity". As an example can we use the place where we have a presence as our "identity"? Is it possible to use it in encryption? Physical presence in a particular position at a specific time can be our "identity" in cryptography [16]. For example, a receiver located at the position A receives a message from a transmitter located at the position B. Specific geographic position can guarantee that the posted message is sent by a transmitter at the position B. Another use would be position based cryptography for access control. For example, a person who is physically present at a specific position can detect the message. For better understanding the issue, first secure positioning in one-dimensional space will be expressed and then we extended the idea into a three-dimensional space.

3.2 Key Exchange Based on Position

As it was described in the previous section, one of the elements which can be used in cryptography is the geographic position as the identity. For the sake of a secure positioning and exchanging the keys based on a positional situation in a two-dimensional environment, the two verifiers V_1 and V_2 and the prover P, which is located between them and lays claim on a valid position, are presumed according to figure 2(a). The verifiers V_1 and V_2 possess the primary key K. The verifier V_1 sends the string X and the verifier V_2 sends the key K to the prover P and these two values meet each other in the position P. As it is seen in figure 2(b), the prover P calculates the value of $PRG(X, K)$ using the semi-random producing function and sends it to V_1. While sending the X string, V_1 has calculated the value of $PRG(X, K)$. So, after receiving this value, it can check its accuracy and confirm receiving the value in a right time [16].

In order to perform security assessment according to the figure 3, two attackers A_1 and A_2 are positioned somewhere between the verifiers and P. The A_2 attacker gets access to the key K earlier than P, but it does not have access to the X string at this moment. The A_1 attacker also accesses the X string sooner than P; however, it does not possess the key K to get reliable information about the X string and so it cannot have a correct understanding of the X string. Assume that the attacker A_2 can possess the key. When the X string reaches it, it can produce the accurate value for $PRG(X, K)$ and dispatch it toward V_1; however, before the message sent from A_2 reaches V_1, the value calculated by P reaches the V_1 as a valid value in a shorter time (valid time), and the invalidity of the message dispatched by A_2 and consequently the invalidity of the place claimed by it becomes evident for V_1 [16].

Now, it is possible to generalize the one-dimensional environment to the three-dimensional environment. As can be seen in figure 1, assume that we have four verifiers named V_1, V_2, V_3 and V_4 and these verifiers can store strings X. We assume that verifiers can communicate through a secure channel. A prover has a presence at position P in the space between verifiers. V_1 can send X_1 and X_5 to the prover P. V_2 can send X_2, V_3 sends string X_3 and V_4 can send X_4 and K_1. The prover generates new K_S serially. The final key is K_6 which is sent from the prover to all verifiers. Because of secure communication between verifiers

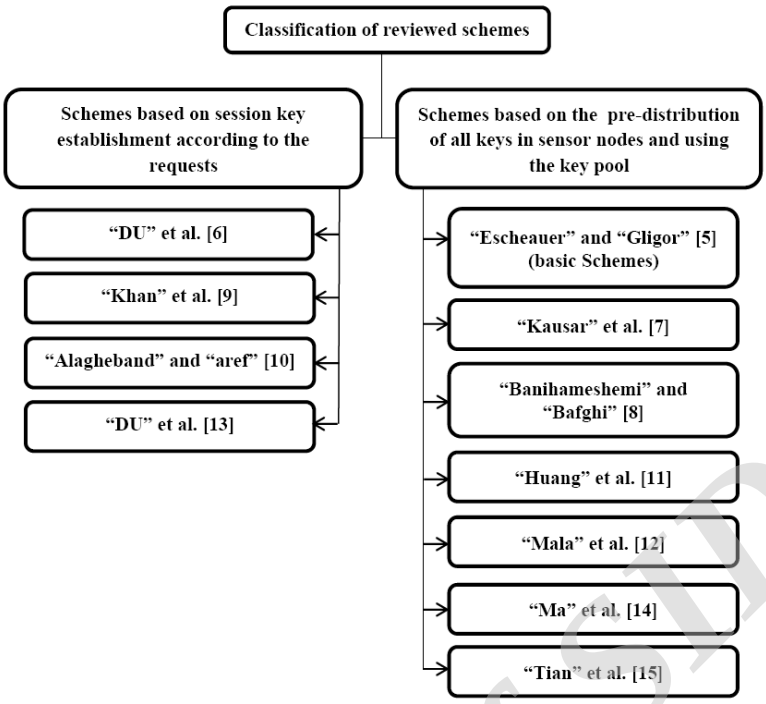

Figure 1. Classification of reviewed schemes.

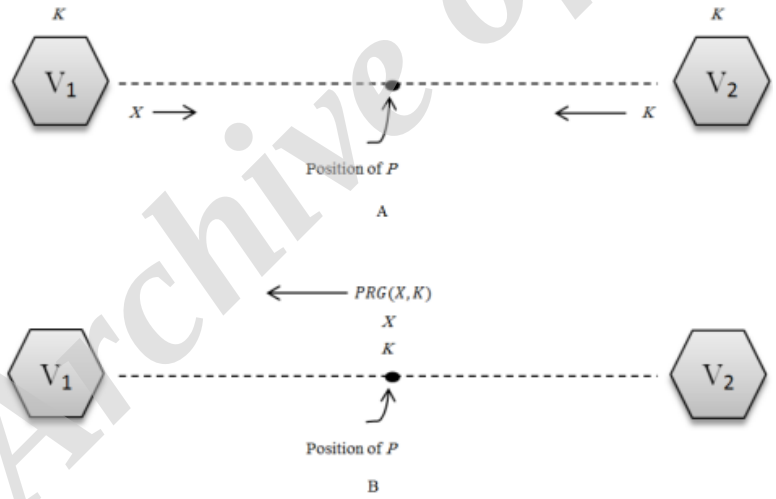

Figure 2. (a) V_1 and V_2 send the values of X and K to P. (b) P sends the value of $PRG(X, K)$ for V_1.

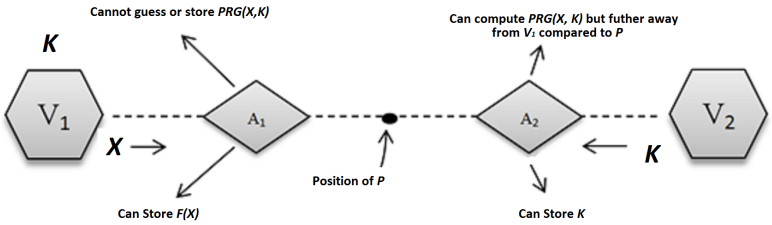

Figure 3. The inability of the attackers in demonstrating the claim that they are located in the P position

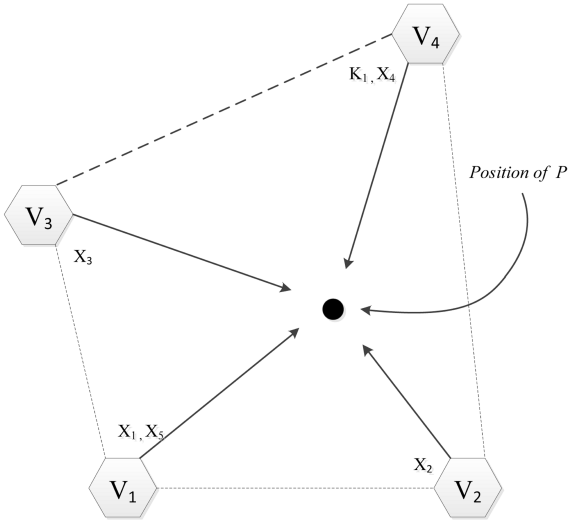

Figure 4. Position-based key exchange in a *3D* environment.

and access to the strings X and K, all of them have generated and gained the K_6 before the prover's calculations. Verifiers compare the received K with their own generated Key and calculate the time of response to verify the claim of the prover. Calculations for the final key K_6 are shown bellow [16, 17]:

$$\begin{aligned} K_2 &= PRG(X_1, K_1), \\ K_3 &= PRG(X_2, K_2), \\ &\vdots \\ K_6 &= PRG(X_5, K_5) \end{aligned} \tag{1}$$

In order to make transparency in the results produced, some assumptions have been made in explicating the cryptography oriented on positional framework. It is assumed that the facilities can read the bits from the strings and immediately conduct the low-weight calculations. Taking into account one protocol with this assumption and compiling it to another protocol which has taken into consideration the time needed for performing the calculations (for reliable facilities) and the time needed for an attacker to perform a precise locating operation is accessible. Similarly, it can be assumed that a legal prover is located in the position which it claims, and the same way, the minute difference in the real position and the purported position can be ignored. Based on the main idea of this compiler, once a message named "m" is received by a legal prover, a constant amount of time would be needed for the performance of the calculations (which is called t) for doing the quick calculations. The time needed for receiving the message m by the prover will be taken equal to T. The time needed for sending the results of the calculations (for example, the final key) on the verifier V_1 is equal to t_1. Therefore, all parts (provers and verifiers) have a delay equal to t for receiving and sending the messages. Therefore, the time

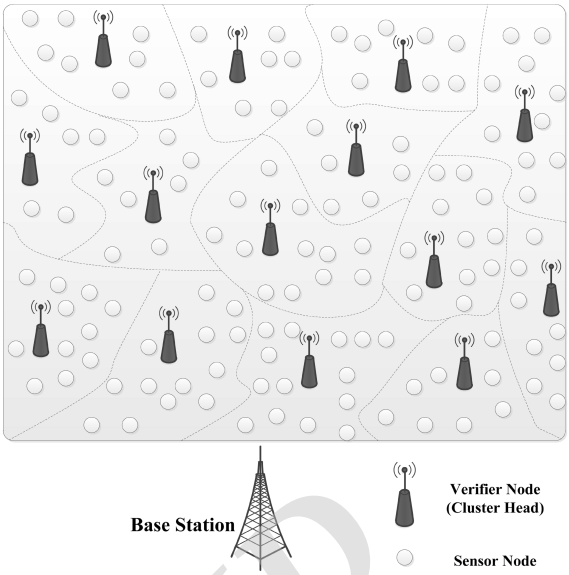

Figure 5. Network model in the proposed scheme.

needed for receiving and sending the messages equals to $T + t + t_1$ [16].

3.3 Assumptions and Terminology

In the proposed scheme, to consider scalability in the network, the structure is considered as a hierarchical network components with clustering that includes a base station (BS) and sensor nodes. There are two types of sensor nodes; verifier nodes (VN) which are actually cluster heads and sensor nodes (SN) which are member nodes. Network model can be seen in Figure 5.

Assumptions made in the scheme:

- BS is impenetrable and there are no limitations in terms of computational resources, energy and storage.
- VNs are equipped with temper-proof hardware. Although they do not have unlimited computing resources, energy and storage such as base station, they are much better than SNs.
- VNs are equipped with GPS system and always are aware of their position.
- Ordinary sensor nodes (SN), are not equipped with temper-proof hardware due to their inherent limitations.
- Each VN and SN has a unique ID.
- VNs do not move and they are in a fixed position, but the sensor nodes are capable of mobility. All SNs and VNs usually spread to areas that cannot be controlled. Each cluster of SNs makes sense of the surrounding environment and sends the recorded raw data to the VN. Each VN collects information and track their BS is determined by specific protocols.

- Until a complete network installation, the adversary does not have enough time to access the network.

For presentation of the proposed model, the statements used for the introduction of the members, components and included elements are listed and summarized in the Table 1.

Table 1. List of used terms and phrases in the proposed scheme.

Description	Notation
BS	Base station
VN	Verifier nodes
SN	Sensor nodes
K	The pre-loaded, joint single key in the VNs
VN_i	i^{th} Verifier node (head-cluster)
ID_i	The identity of the ith verifier node
P_i	The position of the establishment of the i^{th} verifier node
$K_{(}VN_i)$	The key of i^{th} cluster
K'_{VN_i}	The key for a secure relationship between VN_i and BS
$nonce_i$	The random string corresponding to the i^{th} verifier node
$IdRVNN$	The message of identification request for the neighboring VNs
K'_S	Secret key for secure relationship between VN_{i+1} and VN_i
$\alpha\&\beta$	Random strings
P_{ij}	The position of j^{th} SN from the i^{th} cluster at the moment of registration in the i^{th} cluster
SN_{ij}	j^{th} verifier node from the i^{th} cluster
$K_{(SN_{ij})}$	The key for a secure relationship between SN_{ij} and VN_i head-cluster
$IdRSNN$	The message of identification request for the neighboring SNs
γ'_S	Secret key for a secure relationship between SN_{ij} and $SN_{i,j+1}$
PRG	semi-random producer
$HMAC$	The code of originality validation based on the hash function
$Lmessage_i$	The message of leaving the i^{th} cluster
$Jmessage_{i+1}$	The message of joining the $(i+1)^{th}$ cluster

4 Proposed Scheme

In this section, the details of the proposed model will be presented.

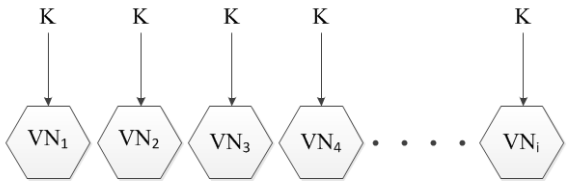

Figure 6. Verifiers node (head cluster) key pre-distribution.

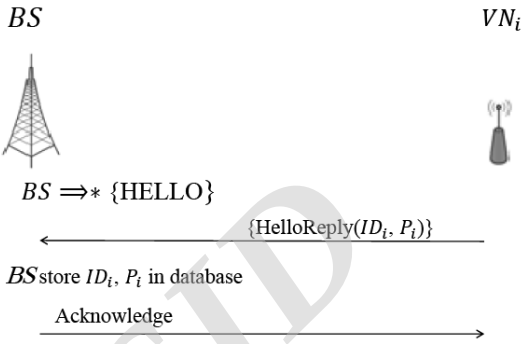

Figure 7. The pre-distribution procedure.

4.1 Key Pre-distribution

In order to minimize the required storage space, in the network pre-deployment phase a single shared key (K) is pre-loaded in all the VNs which is observable in the Figure 6.

4.2 Identification of VNs which are Deployed by BS

After the establishment of VNs in the desired position, the BS broadcasts a "Hello" message in order to identify VNs. In order to ensure that this message will be received by all the VNs, its range is properly considered and will be sent multiple times. After receiving the message, VN_i $(i = 1, \ldots, n)$ response back a "Helloreply" message to the BS for its introduction. The message consist of ID_i $(i = 1, \ldots, n)$ and P_i $(i = 1, \ldots, n)$ that define its position. After receiving P_i and ID_i, BS stores them into a database and then sends a message to VN_i to approve the receipt of P_i and ID_i. This scheme is shown in the Figure 7.

4.3 Connections Between BS and VN

After receiving the approval message from the BS (as shown on Figure 8), the VN constructs K_{VN_i} using a hash function with K and $nonce_i$($K_{VN_i} = H(K, nonce_i)$). Then the VN encrypts the $nonce_i$ using preloaded key K and sends it to the base station. If needed, the base station uses it for providing and comparing with K_{VN_i}. After this step, the pre-loaded key K will be deleted to prevent abuses. VN uses K'_{VN_i} to establish a secure communication with the

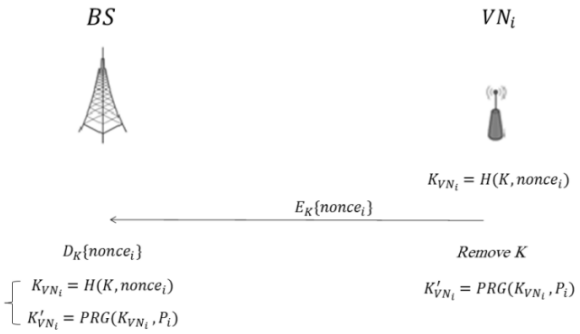

Figure 8. Establishing a secure connection between BS and VN.

BS $(K'_{VN_i} = PRG(K_{VN_i}, P_i))$.

4.4 Identification of Neighbor VNs and VN-VN Connections

In the next step each VN tries to identify its VN neighbors. To do so, the VN broadcasts a message as "Identification Requests for VNs Neighbors" $(IdRVNN)$, which includes its ID. The message is broadcasted in the radius of VN's signal strength. Other VNs after receiving the message reply back and send their ID to the sender of "$IdRVNN$" message. So each VN receives a number of IDs and adds them to the list of its neighbors. VNs must have a secure connection to communicate. For example, consider establishing a secure connection between VN_i and VN_{i+1}. VN_i sends ID_{i+1}, $nonce_i$ and $HMAC_{K'_{VN_i}}$ $(ID_{i+1}||nonce_i||P_i)$ to the BS. VN_{i+1} also sends ID_i, $nonce_{i+1}$ and $HMAC_{K'_{VN_{i+1}}}$ $(ID_i||nonce_{i+1}||P_{i+1})$ to the BS. The BS extracts private key (K'_S) as bellow, and sends it to VN_i and VN_{i+1} to establish a secure connection between them:

$$K_S = PRG(K'_{VN_i}, P_{i+1}) \quad (2)$$

$$K'_S = PRG(K_S, P_i) \quad (3)$$

The BS sends α, $HMAC_{K'_{VN_i}}(K'_S||\alpha||nonce_i||P_i)$, and K'_S to VN_i and also sends K'_S, β and $HMAC_{(K'_{VN_{i+1}})}$ $(K'_S||\beta||nonce_{i+1}||P_{i+1})$ to VN_{i+1}. α and β are random strings. The procedure of performing this stage is shown in the Figure 9.

4.5 Cluster Establishment and VN-SN Communications

For the clustering and registering SNs in clusters with VNs as their cluster head, first the SNs broadcast a "Hello" message that contains their ID. The wireless communication radius of the SN and the network structure is such that this message is received by multiple VNs. In the proposed scheme it is assumed that the message is clearly received by at least four VNs. In order to make sure that the message is received by at least four VNs, the SN can broadcast it several times. VNs which are within the communication radius of the SN receive the "Hello" message and reply back a "HelloReply" message to the SN. The message contains VN's ID and position (P_i). According to the strength of the received signal and the time taken to get response from the VNs, the SN makes a list of them. The VN which has the strongest signal and actually is the nearest VN to the SN, will be the cluster head in the above list. Other VNs in the list are cluster heads of other SNs. They are verifiers for the key exchange and considered as a backup cluster headers if the SN leaves the current cluster. The SN having the position of the four VNs and calculating the time of response of the "Hello" message, and then calculating its distance from each of the VNs defines its position and calls it P_{ij}. Actually it is the position of the j_{th} SN from i_{th} cluster at the moment of registration in the i_{th} cluster and sends P_{ij} to VN_i. The key $K_{SN_{ij}}$ is calculated and constructed as you can see in Figure 10. The key is considered to establish a secure connection between SN_{ij} and VN_i in cooperation with the backup cluster headers.

4.6 Identification of Neighbor SNs and SN-SN Connections

In this step SNs attempt to identify other neighbor SNs in the same cluster. Each SN broadcasts a message as "Identification Requests for SNs Neighbors" $(IdRSNN)$ in a short range within the cluster. The message contains SN's ID. Other SNs after receiving this message, respond back their ID to the sender of "$IdRSNN$". So each SN receives the respond of other SNs which includes their ID and adds them to the list of its neighbors. In order to establish a secure communication between two SNs of a cluster, a secret key must be assigned to do this. Assume SN_{ij} and $SN_{i,j+1}$ want to communicate with each other. To do so, the SN_{ij} sends $ID_{i,j+1}$, $nonce_{ij}$ and $HMAC_{K_{SN_{ij}}}(ID_{i,j+1}||nonce_{ij}||P_{ij})$ to VN_i and $SN_{i,j+1}$ sends ID_{ij}, $nonce_{i,j+1}$ and $HMAC_{K_{SN_{i,j+1}}}(ID_{ij}||nonce_{i,j+1}||P_{i,j+1})$ to VN_i. VN_i extracts the private key γ'_S and gives it to SN_{ij} and $SN_{i,j+1}$ to establish a secure connection between them:

$$\gamma_S = PRG(K_{SN_{ij}}, P_{i,j+1}) \quad (4)$$

$$\gamma'_S = PRG(\gamma_S, P_i) \quad (5)$$

To do so, VN_i sends $nonce_i$, $nonce_{ij}$, γ'_S, and $HMAC_{K_{SN_{ij}}}(\gamma'_S||nonce_i||nonce_{ij})$ to SN_{ij}. VN_i

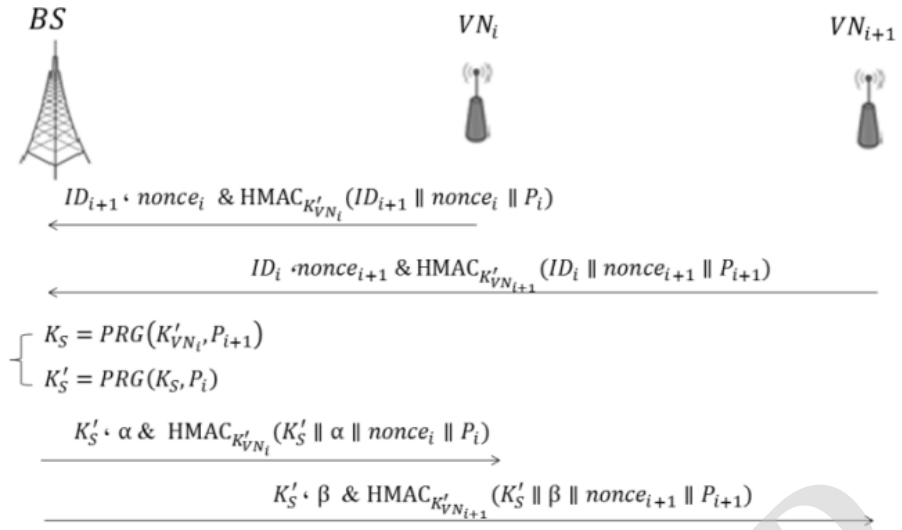

Figure 9. Establishing a secure connection between two head clusters.

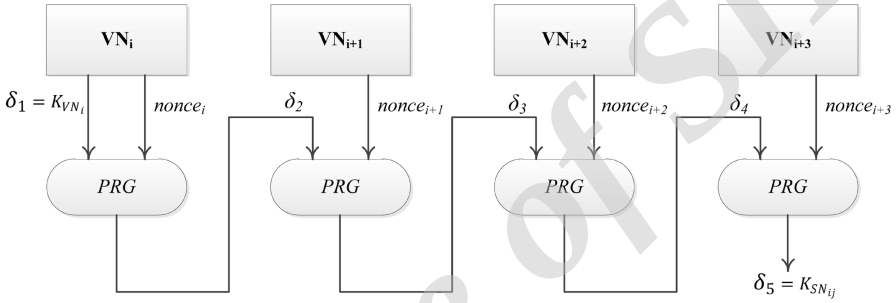

Figure 10. Allocating $K_{SN_{ij}}$ using four verifiers.

also sends $HMAC_{K_{SN_{i,j+1}}}(\gamma'_S||nonce_i||nonce_{i,j+1})$ to $SN_{i,j+1}$, γ'_S, $nonce_i$, and $nonce_{i,j+1}$. Up to This step, through the position of appropriate keys to the connection, the communications between cluster heads and the base station, cluster heads and cluster heads, cluster head and sensor nodes and two sensor nodes have been made secured. The procedure of performing this stage is observable in the Figure 11.

4.7 Key Revocation and Adding a new Key

In the specific period of time called T, each VN publishes a message of the declaration of its status including its ID, and the SN receives it and by observing the ID of its head-cluster, informs its VN of its being alive through responding to this message. If a SN does not send a response to its head-cluster, after the time period of $3T$, that is three times of the public announcement of the declaration of the status of VN, the SN would be considered as a node whose life has ended and all of its keys will be revoked and termination of the node will be informed to the BS.

In another state, when the node is compromised (the base station is responsible for identifying and announcing infiltration), BS sends a revocation message and informs the head-cluster and the supporting VNs of the identity of the compromised SN. The head-cluster also informs the neighboring SNs of the identity of the compromised node. After VNs and SNs related to the compromised node receive the revocation message, they revoked all the keys they had developed for their relationship with the nodes and this way, the compromised node would leave the network.

The dynamic topology of the sensor networks is an essential part of them, because the nodes can be added or removed; so the proposed model should permit the nodes to be added or removed. It is assumed that a new SN intends to be added to the network. Through a "Hello" message, the SN publicly announces its identity and the request for joining the network. The intensity of the signal imparted is such that it will be received by at least four VNs. The VNs which receive this message will send the response containing

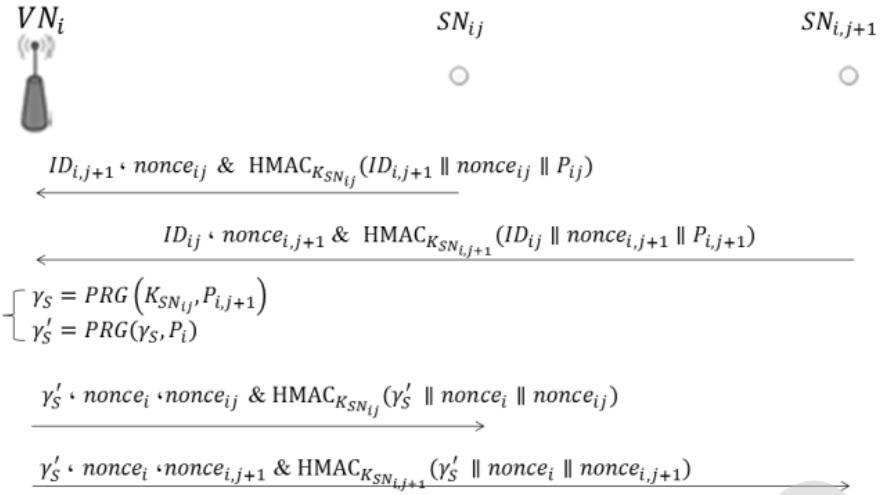

Figure 11. Establishing a secure connection between two sensor nodes in a cluster.

their identity to a new SN. It is noteworthy that the VNs get assured about the legality of the new SN through a secure channel with BS and with each other. Once SN selected the list of four main VNs and the supporters based on the intensity of the signal received by them and selected their distance from them, it will be joined by the cluster and establish its private key with the VN in a mechanism that is similar to what has been described under the subsection 4.5.

4.8 Leaving the Cluster and Joining a new Cluster

As it was noted previously, each VN publicly releases a message of status declaration containing its ID in the specific time period T and the SNs receive the message and inform their VN of their being alive after seeing the ID of their head-cluster. If the signal which a SN receives from another VNs is stronger than the signal which is received from its head-cluster, it means that the moving SN is leaving its cluster and entering the limits of another head-cluster. Therefore, SN updates the list of four of its head-clusters and attempts to change its head-cluster. For this purpose, SN_{ij} sends the values of $ID_{i,j}$, ID_{i+1}, $nonce_{ij}$ and $HMAC_{K_{SN_{ij}}}(ID_{i,j}||ID_{i+1}||nonce_{ij})$ within the cluster leaving message $Lmessage_i$ to VN_i and sends the same values through a message of joining the $i+1$ cluster called $Jmessage_{i+1}$ to VN_{i+1}. Through a secure channel with VN_{i+1}, VN_i sends the hash values to it. VN_{i+1} compare the values received from VN_i with the hash values received from SN_{ij} and if these two values are equal and the confirmation message is sent to VN_i and SN_{ij}, it removes the previous head-cluster for SN_{ij} and the relevant keys and informs BS of this action. Subsequently, VN_{i+1} has incorporated this moving cluster in its own cluster and informs the BS of this development. After the incorporation of the node in the new cluster, given its new positional position and the four VNs, which are situated in its list of verifiers, the steps taken for the position of new keys for this moving node would be repeated.

5 Evaluating the Proposed Model

After presenting the proposed model in the previous section, in this section, the model is assessed and evaluated in terms of security factors and memory complexity.

5.1 Security Assessment

Since the basis of the identity of the network components is oriented on their position, and given the cryptography techniques based on positional position and the principle of secure position, which were foreseen in the proposed model, this model provides a suitable security as compared to the other models. This is because contrary to the other models in which the attacker was able to infiltrate into the network through accessing the primary keys or the pre-loaded keys, in proposed model, the attacker needs the demonstration of a valid situation as a parameter for producing communicative keys and this procedure is impossible in the proposed model given the procedure which was noted in the discussion over position. However, with the aim of assessing the security, the resistance and flexibility of the proposed model over some of the well-known attacks on the sensor networks would be investigated.

5.1.1 Sinkhole Attack

As previously mentioned, the main goal of the sinkhole attack is to attract the whole traffic from a specific region by creating a black hole in the network. If a VN illegally claims that it is located in a valid position and tries to move the traffic by deceiving the network's SNs, first it should have access to the pre-loaded key K, and as it was noted, this key has been removed for the VNs in after-production stage and the attacker does not have access to it. suppose the attacker has accessed this key through claiming a valid situation, and tries to introduce itself as a valid head-cluster for the neighboring VNs and BSs. As it is shown in the Figure 4, the claim laid by the verifier and his invalid positional position has been determined and BS is informed about it. Similarly, whenever an illegal SN decides to register in a cluster with a claim of having a valid place, using the mechanism put forward in the proposed model and the four key verifiers, it will not be allocated to it and the mendacious allegation of its presence in a valid place will become obvious and BS will soon be informed.

5.1.2 Wormhole Attack

The other type of attack is wormhole attack whereby the attacker receives the packages from a specific place and then transfers them to another place in the network by making a tunnel throughout a link with small coverage which will be controlled by the attacker itself and pretends to be providing a reliable service. As it was noted in the sinkhole attack, when the attacker attempts to move the network's traffic, given the proposed model, it will not be successful. The mechanism for confronting this threat is similar to the mechanism for confronting the sinkhole attack.

5.1.3 Node Capture Attack

The node capture attack is another group of attacks in which the attacker physically accesses the sensor and brings it under its complete control. Since the sensor nodes are usually located in an environment far away from the network administrator, an attacker can take part physically and capture some sensor nodes through physical attacks and then decrypt them. To carry out the node capture attack, the attacker completely takes over the hardware using the physical access. However, since in the proposed model, the VNs have some kind of a hardware resistant against violation, the attacker would not be able to take over them. However, decrypting a SN through node capture attack seems more probable because this group of nodes are not equipped with a hardware resistant to encroachment and manipulation.

Given the procedure which is stated for destroying the key in the compromised nodes, if an attacker takes over a SN, all of its communicative keys will be destroyed by the network and the node will be eliminated from the network and the whole network will be immune to infiltration. Therefore, with this attack, only the captured node will be removed from the network which is ignorable in the scale of a great amount of sensor nodes.

5.1.4 Masquerade Attack

In this kind of attack, an attacker can claim that a node is valid and has a share in the network communications. Since in the proposed model, all the sensor nodes are validated based on their positional position in at the moment of registration in their cluster, the node which is entered into the network by the attacker will not have the capability of infiltration and getting involved in the network because it lacks valid primary information. From the other hand, all the neighboring nodes which are involved in the communicative networks will be identified and qualified in the phase of identifying the neighbors; so an attacker cannot claim that it was a valid node and then exchange false information with a legal node on this basis.

5.1.5 DOS Attack

Denial of service attack is a form of attack in which the attacker somehow tries to make some parts of the network inaccessible, the whole network or a considerable part of the network. For example, an attacker can create a fake destruction message and disseminate it into the network and nullify a considerable number of the sensor nodes and practically interrupt the activities of the network. In order to confront this the destruction message, which is broadcast for the sensor nodes in the network, includes an originality validation code. Therefore, the fake messages whose originality is not validated for the sensor knots will be rejected.

5.2 Assessment from the Viewpoint of Storage Costs

Given the essential limitations of the sensor nodes, the models of key management should take into consideration the storage costs for the pre-distribution of the primary keys in the sensor nodes. As a result, the effectiveness of the proposed model is compared to the viewpoint of space needed for storage with a number of other schemes. In the base model which is in fact a model for the homogeneous sensor networks, by presuming N normal sensor nodes existing in the network and pre-loading of keys in each of these nodes, the storage space needed is equal to [5]:

$$Storage\ space\ for\ basic\ scheme = a.N \quad (6)$$

In the model put forward by Kausar *et al.* [7], M values have been considered as the number of H sensors, and N has been considered as the number of L sensors. By taking into consideration that in each L sensor, a productive keys and in each H sensor, b productive keys have been pre-loaded, then the number of pre-loaded keys in the network would equal to:

$$Storage\ space\ for\ Kausar\ scheme = a.N + b.M \quad (7)$$

The possibility of sharing a similar key between the Kausar model and the base model would be accessible by loading only two productive keys in the L sensors as compared to the loading of 100 productive keys in the normal sensors in the base model. For example, there are 1000 units of L sensors and 10 units of H sensors in a HSN in such a way that each L sensor would be pre-loaded by two productive keys and each H sensor would be pre-loaded by 100 productive keys. The amount of memory needed for the Kausar model throughout the key length unit equals $2 \times 1000 + 100 \times 10 = 3000$, while for the base model which belongs to a homogeneous network in which 1000 normal sensors each of which are loaded by 100 keys, there is a space of $100 \times 1000 = 100,000$ which is 33 times larger than the Kausar model [7]. It is noteworthy that in the model proposed in this work, we have used the parameter of positional position as the raw material for encryption where only M units of K key have been pre-loaded through the whole network which means that one key for each verifier node or the head-cluster.

According to the example above and by taking into consideration 10 head-clusters, we will only need to store 10 single keys through the whole network and this reduction in the amount of keys needed for pre-loading will provide us with a remarkable economization as compared to the base model and Kausar model.

In the key management scheme presented by Ullah Khan *et al.* [9], each moving node is pre-loaded with three keys (SK keys, K_{plc} keys and originality validation key) and each group will be pre-loaded with six keys (BS general key, its own public/private couple keys, SKG, $CNDK$ and K_{prt}) and by taking into consideration the M values as the number of head-clusters and N as the number of moving sensors, the number of pre-loaded keys would be equal to [9]:

$$Storage\ space\ for\ Ullah\ Khan\ scheme = 3.N + 6.M \quad (8)$$

Now by taking into consideration 10 head-clusters and 1000 moving nodes, the space needed for storage in the key length unit in Ullah Khan's key management scheme would be equal to $3 \times 1000 + 6 \times 10 = 3060$, while having a low cost against the homogeneous networks in terms of the memory space needed, is far away from the results achieved in the proposed model.

6 Conclusion

In this work, a novel key management in the heterogeneous sensor networks based on the position of nodes is presented. In this protocol position based cryptography and its assumption were applied to build connection rules between the base station and the verifier nodes, verifier nodes with each other, verifier nodes with the cluster members, and the members inside the cluster with each other. Our model is easy to implement for applications such as smart control system of containers in the ports and decks in the industry of ports and maritime. The presented communication protocol has secured the sensor network and a mechanism was declared for scalability of the network and supporting the movement of the sensor nodes. Finally, the model was evaluated from a security point of view and memory complexity. The evaluation results show that the proposed security model have strong resistance to well-known sensor network attacks, and its memory complexity is suitable for low resource sensor nodes.

Acknowledgement

The authors would like to thank Ports and Maritime Organization(PMO) for their research scholarship.

References

[1] Javier Lopez, Jianying Zhou, "Wireless sensor network security", IOS Press, Amsterdam, 2008.

[2] Ian F Akyildiz, Weilian Su, Yogesh Sankarasubramaniam, Erdal Cayirci, "Wireless sensor networks: a survey", Published by Elsevier Science B.V., Computer Networks, Vol.38, pp. 393422, 2002.

[3] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey", Computer Networks, Vol.52, issue 12, pages: 22922330, 2008.

[4] Yuan Xue,"Key Management Schemes for Distributed Sensor Networks", PhD thesis, The University of Western Ontario, London, 2008.

[5] Laurent Eschenauer, Virgil D. Gligor, "A key-management scheme for distributed sensor networks", In proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41-47, New York, 2002.

[6] Dahai Du, Huagang Xiong, Hailiang Wang, "An Efficient Key Management Scheme for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, Vol.2012, Article ID 406254, pages: 1-14, 2012.

[7] Firdous Kausar, Sajid Hussain, Laurence T. Yang, Ashraf Masood, "Scalable and efficient key management for heterogeneous sensor networks", The Journal of Supercomputing, Vol.45, pages: 44-65, 2008.

[8] Saber Banihashemian, Abbas Ghaemi Bafghi, "A new key management scheme in heterogeneous wireless sensor networks", ICACT'10 Proceedings of the 12th international conference on Advanced communication technology Pages 141-146, Gangwon-Do, South Korea, February 07 - 10, 2010

[9] Sarmad Ullah Khan, Claudio Pastrone, Luciano Lavagno, Maurizio A. Spirito, "An Energy and Memory-Efficient Key Management Scheme for Mobile Heterogeneous Sensor Networks", In Proceedings of 6th International Conference on Risks and Security of Internet and Systems (CRiSIS), pp. 1-8, Timisoara, 2011.

[10] Mehdi Ramezan Alagheband, Mohammadreza Aref, "A Secure Key Management Framework for Heterogeneous Wireless Sensor Networks", In proceedings of Communications and Multimedia Security Lecture Notes in Computer Science, Vol.7025, pages: 18 31, Ghent, 2011.

[11] Jen-Yan Huang, I-En Liao, Hao-Wen Tang, "A Forward Authentication KeyManagement Scheme for Heterogeneous Sensor Networks", EURASIP Journal on Wireless Communications and Networking, Vol. 2011, Article ID 296704, pages: 1-10, 2011.

[12] Boushra Maala, Yacine Challal, Abdelmadjid Bouabdallah, "HERO: hierarchical key management protocol for heterogeneous wireless sensor networks", in IFIP International Federation for Information Processing, Vol. 264, pages: 125136, Boston, 2008.

[13] Xiaojiang Du, Mohsen Guizani, Yang Xiao, Hsiao-Hwa Chen, "A Routing-Driven Elliptic Curve Cryptography Based Key Management Scheme for Heterogeneous Sensor Networks", IEEE Transaction on Wireless Communications 8(3), Pages: 1223 - 1229, 2009.

[14] Chunguang Ma, Zhiguo Shang, Huiqiang Wang, Guining Geng, "An Improved Key Management Scheme for Heterogeneity Wireless Sensor Networks", Mobile Ad-Hoc and Sensor Networks, LNCS 4864, pp. 854865, Springer-Verlag Berlin Heidelberg , 2007.

[15] Biming Tian, Song Han, Tharam S. Dillon, "A Key Management Scheme for Heterogeneous Sensor Networks Using Keyed-Hash Chain", Fifth International Conference on Mobile Ad-hoc and Sensor Networks, 2009.

[16] Nishanth Chandran, Vipul Goyal, Ryan Moriarty and Rafail Ostrovsky, "Position Based Cryptography", In Proceedings of 29th Annual International Cryptology Conference (Crypto 2009), Vol.5677, pages: 391-407, Santa Barbara, 2009.

[17] Giovanni Di Crescenzo, Richard Lipton, Shabsi Walfish, "Perfectly secure password protocols in the bounded retrieval model", In Proceedings of Third Theory of Cryptography Conference, Vol. 3876, pages: 225-244, 2006.

[18] Jeremy Ribeiro, Le Phuc Thinh, Jedrzej Kaniewski, Jonas Helsen, Stephanie Wehner, "Device-independence for two-party cryptography and position verification", arXiv:1606.08750, 2016.

[19] Piotr Bilskia, Wiesaw Winieckia, "Analysis of the position-based quantum cryptography usage in the distributed measurement system", Measurement 46, pages: 43534361, 2013.

[20] JunWei Zhang, JianFeng Ma, Cjao Yang, Li Yang, "Universally composable secure positioning in the bounded retrieval model", Science China Information Sciences, Vol. 58, Issue 11, pages: 115, November 2015.

[21] Yingpei Zeng, Jiannong Cao, Jue Hong, Shigeng Zhang, Li Xie, "Secure localization and location verification in wireless sensor networks: a survey", The Journal of Supercomputing, Vol. 64, Issue 3, pages: 685701, June 2013.

[22] Taha Yasin Rezapour, Meer Soheil Aboalghasemi, Reza Ebrahimi Atani, "Secure Positioning for Shipping Containers in Ports and Terminals Using WSN", 11th International ISC Conference on Information Security and Cryptology (ISCISC14), Univesity of Tehran, Pages: 10 14, 2014.

[23] Mei-jiao Duan, Jing Xu, "An efficient location-based compromise-tolerant key management scheme for sensor networks", Information Processing Letters, Volume 111, Issue 11, Pages: 503-507, 15 May 2011.

[24] Amir Hassani Karbasi, Reza Ebrahimi Atani, "Projective plane-based key pre-distribution by key copying and exchanging based on connected dominating set in distributed wireless sensor networks", International Journal of Information and Communication Technology, Vol. 9, Issue 4, Pages: 438-462, 2016.

[25] Taha Yasin Rezapour, Meer Soheil Abolghasemi, Reza Ebrahimi Atani, "A position-based key management scheme for heterogeneous sensor networks", 10th International ISC Conference on Information Security and Cryptology (ISCISC13), Pages: 1-6, 2013.

[26] Yanchao Zhang, Wei Liu, Wenjing Lou, Yuguang Fang, "Location-based compromise-tolerant security mechanisms for wireless sensor networks", IEEE Journal on Selected Areas in Communications, Vol. 24 (2), Pages: 247260, 2006.

Taha Yasin Rezapour obtained his B.S. and M.S. at the University of Guilan, Rasht, Iran. He got his B.S. degree in 2008 in electronics engineering and his M.S. in IT engineering in 2013. He is a member of Iranian Society of Cryptology (ISC). He is now working for Ports and Maritime Organization(PMO). His main research interests include, network security, symmetric cryptography, position-based cryptography, WSN security and VMware security.

Reza Ebrahimi Atani studied electronics engineering at the University of Guilan, Rasht, Iran and got his B.S. degree in 2002. He followed his M.S. and Ph.D. studies at Iran University of Science & Technology (IUST) in Tehran, and received the Ph.D. degree in 2010. He isholding an associate professor position in department of computer engineering at the University of Guilan. He is a member of IEEE, IACR and also Iranian Society of Cryptology (ISC). His main research interests focuses on design and implementation of cryptographic algorithms and protocols as well as their applications in computer and network security and mobile communications.

Meer Soheil Abolghasemi obtained his B.S. in software engineering at Lahijan Azad University in Lahijan, Iran. He received his B.S. degree in 2008. He pursued his Masters study at the University of Guilan in Rasht, Iran and received his M.S. degree in E-Commerce in 2013. He is now working in MTNI telecommunication company in Tehran. His main research interests include position-based cryptography, network security, cloud computing security, WSN security and payment security.

The ISC Int'l Journal of Information Security
ISeCure

July 2016, Volume 8, Number 2 (p. 165)
http://www.isecure-journal.org

Persian Abstract

یک طرح مدیریت کلید نوین برای شبکه‌های حسگر بی‌سیم ناهمگن بر اساس موقعیت گره‌ها

طاها یاسین رضاپور[۱،۲]، رضا ابراهیمی آتانی[۱] و میرسهیل ابوالقاسمی[۱]

[۱] دانشکده مهندسی کامپیوتر، دانشگاه گیلان، رشت، ایران

[۲] دانشکده فناوری اطلاعات، سازمان بنادر و دریانوردی، تهران، ایران

شبکه‌های حسگر بی‌سیم دارای کاربردهای متنوعی در حوزه‌های تجاری، نظامی، پزشکی و محیط‌زیست می‌باشند. با توجه به استقرار گره‌های حسگر کم‌هزینه با منابع انرژی محدود، این شبکه‌ها با چالش‌های امنیتی فراوانی روبرو هستند. یک رویکرد اساسی برای آماده‌سازی ارتباطات بی‌سیم امن در WSNها به‌کارگیری یک پروتکل مدیریت کلید رمزنگاری کارآمد برای حصول بالاترین امنیت با کمترین هزینه می‌باشد. انگیزش اصلی این مقاله به‌کارگیری موقعیت گره‌های حسگر به‌عنوان جزئی از هویت به‌منظور مدیریت کلید در شبکه‌های حسگر ناهمگن می‌باشد. در طرح ارائه‌شده موقعیت گره‌های حسگر به‌عنوان جزئی از هویت برای احراز اصالت و تخصیص کلید برای تمامی ارتباطات شبکه بکار گرفته‌شده است. در مقایسه با سایر طرح‌های ارائه‌شده تکنیک پیشنهادی سطح بالاتری را از نظر مقیاس‌پذیری، امنیت، انعطاف‌پذیری و پیچیدگی حافظه کمتر ارائه داده است.

واژه‌های کلیدی: رمزنگاری مبتنی بر موقعیت مکانی، رمزنگاری، مدیریت کلید، شبکه‌های حسگر ناهمگن.