P- ISSN 1991-8941 E-ISSN 2706-6703 *Journal of University of Anbar for Pure Science (JUAPS)* Open Access
2012,(6), (2) :58-64

Key Management Scheme for Mobile Wireless Sensor Networks

Foad Salem Mubarek * **Sufyan T. Faraj ****

*University of Mosul - College of Computer Science and Mathematics.
**University of Anbar - College of Computer.

ARTICLE INFO

Received: 00 / 00 /00
Accepted: 00 / 00 /00
Available online: 9/12/2012
DOI: 10.37652/juaps.2012.63239

Keywords:
Clustering;
key management;
mobility;
security;
wireless sensor network.

ABSTRACT

Wireless sensor networks (WSNs) are infrastructure-less and resource constraint networks composed of many sensor nodes. These sensors collect information from the area of sense and deliver that information to the base station. WSNs are usually deployed in unattended environment and like other networks need to be secured. In order to secure WSNs, firstly cryptography keys must be distributed in a secure and robust way. Key management problem is rapidly studied in the static WSNs, but it has not been studied thoroughly in mobile (or dynamic) WSNs. When mobility is introduced within WSNs, many challenges and new characteristics appear in the security model. Security requirements for mobile WSNs include authentication, confidentiality, and integrity. The key management scheme represents the corner stone for achieving security services. In this paper, we propose a key management scheme for mobile WSNs which based on track-sector clustering in the roaming area. The proposed system is relying on symmetric cryptography for achieving its goals. The paper represents a work-in-progress report on our advance in the development of this proposal.

INTRODUCTION

Wireless sensor networks (WSNs) consisting of resource constrained sensor nodes have got a special attention in the last decades in the literature. This is mainly due to the widespread of their applications (military and civilian). Sensor nodes of the network collect and send data to the sink, also called base station. The nodes and base station can be either static or mobile depending on the applications and environment conditions. However, most of the previous work on WSNs available in the literature assumes the more convenient case of static WSNs (i.e. with no mobility). Growth in the use of wireless sensor nodes in a hostile environment imposes effective security mechanisms in their design. WSNs have the same challenges as traditional networks but with limited processing power, bandwidth, and energy.

As many of the traditional security techniques are unsuitable for WSNs. It's important to provide security mechanisms for WSN like other kinds of networks.

The main goal of fulfilling security requirements of WSN is to have robust and efficient cryptographic key distribution and management. There are different schemes for key distribution in WSNs, such as matrix-based schemes, polynomial-based schemes, probabilistic-based scheme, and location-based schemes. Good surveys on the issue of key distribution in WSNs can be found in [1, 2].

* Corresponding author at: University of Mosul - College of Computer Science and Mathematics .E-mail address: *fualku1968@yahoo.com*

Most of the previous schemes proposed for key distribution in WSNs were designed explicitly for static WSNs. Adding mobility to WSNs causes emerging new challenges. Thus, the key management will become more complicated when the network contains sensors and/or a base station in a movement manner. Some of these challenges are the open network architecture, shared wireless medium, resource constraints, scalability, and highly dynamic network topology [3]. Hence, existing key distribution schemes for static WSNs cannot be applied directly to mobile sensor networks. The sensors tend to move in any direction making key distribution more complex. So, the base station which actually monitors the network has to have the idea of where each sensor is and with what other sensors it has to share keys in order to have secure communications.

In the beginning of our work in developing this proposed key management scheme for WSNs with mobility capabilities, two important decisions have been taken. The first is choosing a suitable mobility model that facilitates the requirement for movement approach. This must be application-specific like battle field or other applications. Thus, the model in [4] has been selected in our work. The reason for selecting this approach is that the movement for sensor nodes or base station can be predictable at any time and this feature may be suitable for battle field or other similar environments. The second decision is related the issue of clustering formation. In this latter case, we have selected the track-sector partitioning approach [5]. This approach leads to saving energy for the whole network

members and improve the security of the network. Also, this approach helps to distribute the key between the members in efficient way. This approach was previously used in static WSN. In order to efficiently use it in mobile environments, some modifications are required to be introduced. Thus, considering the cluster heads, we have divided the cluster head in to two nodes: data cluster head and routing cluster head.

The rest of the paper is organized as follows: Section 2 represents a survey on some related earlier work in the field. Then, our proposed scheme for key management is described in Section 3. This includes various issues like the mobility model, clustering, key establishment, and the issue of adding and deleting of nodes. Next, a brief security analysis is introduced in Section 4. Finally, the paper is concluded in Section 5.

RELATED WORK

The most widely used approach for key distribution in WSNs is probabilistic key distribution. This approach was firstly introduced by Eschenauer and Gligor [6]. In such approach, there is a global pool key composed of random keys and their identifiers. The key size of the key pool can be 10,000-100,000 keys. Sensors are preloaded with randomly selected keys chosen from the global key pool before they are deployed. These keys form the key chain. In the area of sense, the sensor nodes find out if they have shared keys with the neighbors in order to establish pairwise keys.

The Q-composite technique proposed by Chan et al.[7] improved the original scheme by extending the idea of Eschenauer and Gligor to overcome the difficulties when two sensors do not share a common key.

Liu et al.[8] proposed group based key-distribution scheme. This scheme has two parts: The first one is group-based version of the Eschenauer and Gligor scheme. In this case, the key pool size at any instance of time is 500 and each sensor node randomly selects 50 keys each from in-group and cross-group instance. The second one is a group based scheme that uses a 49 degree bivariate polynomial. Polynomial share from in-group and cross-group is assigned to each sensor node.

Shen et al. [9] proposed a scheme which divides the entire network in to clusters and each cluster has a head node. This scheme uses LEACH protocol in electing new cluster heads (Cluster head is an ordinary node which can communicate with the base station and other cluster head in single hops).

There are also some schemes that used location information of the nodes along with the key distribution schemes explained above. One of these methods is that due to Deng et al. which uses probabilistic approach. This approach divides the global key pool and the deployment area into zones and pre-distribute keys to nodes such that nodes which will be neighbours will get the keys from the same pool and will have higher chance of having common key [10].

There are many other works, like [11, 12, 13] which make use of the location information to solve key distribution problem. Generally location based schemes are highly sensitive to node mobility. As the node is moving in the environment, neighbouring relationship will change and most of the keys which are selected from zone-based key pools become useless. Thus, some careful treatment is needed in order to extend such schemes into mobile environment. Kifayat et al. [14] proposed group-based key management for mobile sensor nodes where the network is divided into groups. Key ring k, from pool of key S, are loaded in to static and mobile sensors in pre-deployment phase in a similar fashion as employed in [6]. Mobile nodes roam in the network and establish connection with at least one sensor in each group with a certain probability within its communication rang.

There are limited works in the literature for key distribution schemes in mobile sensor nodes, which are designed mainly for static WSN and can also be used for mobile sensor nodes like the works in [15, 16, 17].

THE PROPOSED SCHEME

In this paper, we propose a perfectly resilient key distribution scheme for Mobile WSNs. The network is assumed to be composed hundreds of sensor nodes. Sensors are connected to each other wirelessly. Sensors are disposable and thus they are relatively inexpensive. They are also resource constraint; limited in their memory, processing ability, and limited in power. We also assume that the power communication radio for sensors are controlled, which means that sensors have dual radio communications, one for short rang and other for long range [18]. This feature is important for saving energy during intra-clustering (i.e., short rang) and inter-clustering (i.e., long range) communications. These two kinds of communications are both supported by hardware devices. Depending on the role (ordinary nodes or cluster head nodes) of sensor nodes, the radio communication is switched on from one to another. We assume that the time division multiplexing (TDM) is used for communication in the each cluster.

Indeed, it is assumed also that a powerful computer acts as a base station which is considered resourceful, reliable, and has the property of recharging its battery when it is necessary. The base station collects location information from sensors in the field area whenever required. It is assumed that the base station is temper-proof resistance and cannot be captured by an attacker. However sensors can be captured by an attacker. The system model

is considered to be infrastructure less. Sensors are deployed with base station to form network in self-organization manner.

Figure 1 depicted the flow diagram of the proposed scheme with main steps for each phase starts from initialization and assumptions for our model then BS checks and detected changes within interval of time then starts cluster formation, key establishment phase and finally data transmission phase. The network is considered live until sensors dead and the network is stopped.

Mobility Model

The main goal for mobile WSN model is to collect the information from mobile sensor nodes and deliver this information to the base station which is again in movement manner. There are many assumptions that can be proposed to simplify our mobility model. As in [4], our model is considered in a two dimensional rectangular field that sensors deployed in random fashion. Sensor nodes are proposed to be of moderate movement and this movement is caused by another attached device. Thus, energy consumption from this movement is ignored. There is one mobile base station in our model. It is assumed that the sensor nodes can reveal their location information through GPS free solution. The mobile base station can collect location information from the sensor nodes whenever it is required.

We consider that the zone in which the base station moves is known a priori. Also, the location of the base station at certain time is predictable with certain value of probability. Therefore we may assume that the locus of the base station over a span of time is predictable which can be basically a good estimation of the actual movement. The sensor can move in any direction. The location of any sensor at any certain time can be predictable with a certain probability. Therefore it is possible to know the locus of sensor and the base station over a span of time and this is an estimation of the actual movement of the sensors and base station.

In the area of sense, the base station can discover the changes in the network members' locations every interval of time. One interval of time may be defined as the minimum time period that the base station chooses based on the mobility level. The sensor nodes are homogenous and have equal level energy at the beginning.

Our proposed model is closely near to the battlefield environment, where the soldiers and the military vehicles are moving in groups as in Figure 2. These groups are restricts in members which our model proposed and this also meets with military planes.

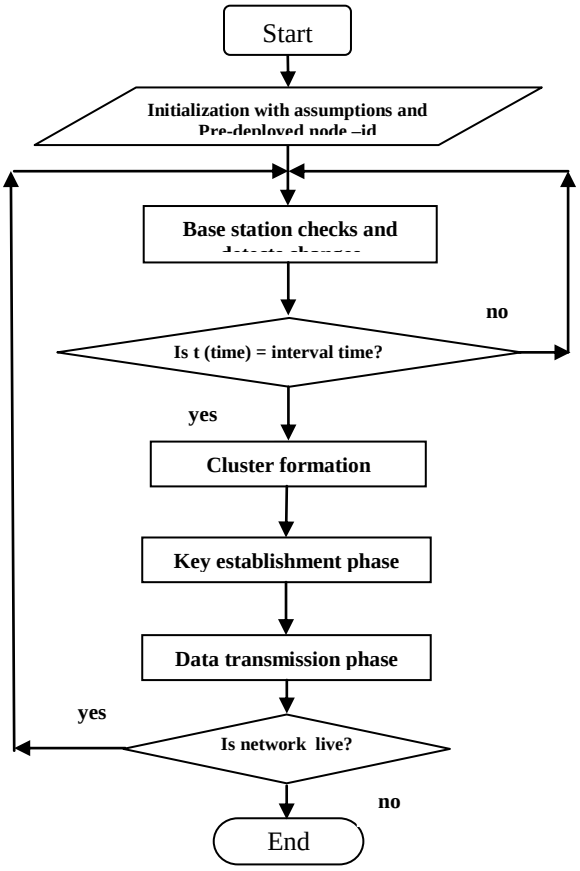

Figure1 Flow-diagram for the proposed scheme

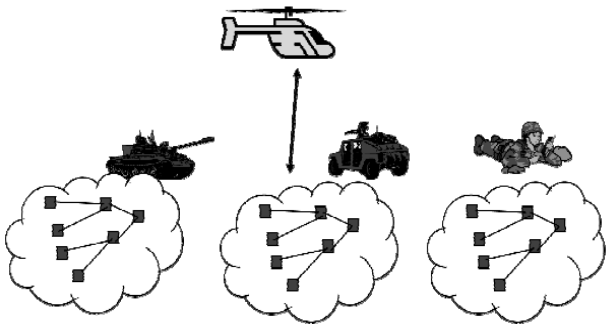

Figure2 Typical battlefield application

Cluster Formation

After deployment of the sensor nodes in the sensor field, network starts clustering configuration. The base station starts dividing the entire sensor nodes into logically hierarchical clustering where each cluster is composed of a group of some sensor nodes. We have adapted the track-sector clustering hierarchical scheme in [5], which was originally proposed for energy efficient routing protocol in static WSNs. We have considered this technique in our work but with some enhancements and modifications.

The proposed track-sector clustering scheme uses tracks and sectors to form clusters. Therefore, a cluster is an area under curved strip formed by intersection of circular track and a triangular sector, as shown in Figure 3. Track1 will serve "routing cluster head" and Track0 would serve as a base station in this context. Tracks are divided into more

sectors. In each sector the nodes communicate with each other as buddy, and to be buddy each node after getting its track-sector information from base station starts "neighbour discovery" phase. The members of a cluster build their neighbour information in "buddy info table" after getting track-sector information from the base station.

For choosing a cluster head (CH) in each cluster, we select an approach that divides cluster head into data cluster head (DCH) responsible for aggregation and fusion the data and routing cluster head (RCH) which is responsible for transformation of the data directly to base station [19]. The reason for that division is to divide the work load into two nodes instead of one.

Division of the network into track-sector and selection of RCH/DCH is the responsibility of the base station. The role of CH is periodical at every interval of time in order to distribute the additional duties to all cluster members and this is done to conserve energy or to increase the longevity of the network.

The base station collects the following information (parameters) from each cluster member: average distance to the base station, remaining energy level, closeness of the neighbor nodes or degree, and the number of times cluster headship already taken. The base station computes credit value for each sensor node in the cluster considering the parameters collected above.

The member with highest credit value is selected as routing cluster head and the second credit is selected as data cluster head. The RCH and DCH should have higher energy, be closer to the base station, higher degree of being directly connected to more nodes, not have taken as members for CH before. In general, the responsibilities of the cluster head are: data aggregation, encrypting the message sent by the nodes that are in the same of its track/sector, communication with the base station, and the key table maintenance.

Key Establishment Phase

Every node in the network is pre-loaded with unique id. After deploying the nodes in the area of sense, the base station (BS) detects the location of the nodes with respect to track-sector (track–id, sector–id), then the base station distributes these information to all nodes in network. At that moment, the nodes at each cluster can compute their own-key and buddy-key and as a result they can get the network key K_n to participate in communication with base station. Also the base station chooses the CH members depending on the credit value, as discussed previously. This information is updated by the base station after regular intervals of time as the nodes move. This time interval is specified by the base station depending on the situation such as the mobility level of the nodes. The following keys can be calculated by every node in the network:

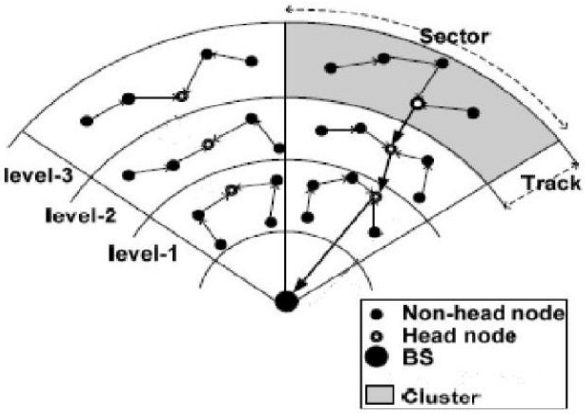

Figure3 Track-sector clustering

- *Buddy key (K_b):* This key is generated by all the nodes after "neighbor discovery" phase is over. It is used to communicate between the nodes which are in the same sector/track, i.e. for node-to-node (N:N) communications. Every node keep "buddy info table" which is the shared keys between cluster members;

$$K_b = id\text{-}sender + f(id\text{-}receiver, track\text{-}id) \quad (1)$$

- *Own key (K_o):* This *key* is initially used by the all nodes. Every node is pre-loaded by a unique id and this key is a function of node-id, sector-id, track-id, and remaining energy in the node. This key used for N:BS communication;

$$K_o = f(node\text{-}id\ ,\ sector\text{-}id\ ,\ track\text{-}id,\ remaining\ energy) \quad (2)$$

- *Broadcast key (K_c):* When CH members are authenticated to base station, they are requested to use this key. Thus, it used for CH:BS communications.
- *Network key (K_n):* After *authentication* is over, all the nodes will gets this key. New nodes to join the network need to use their own-key to encrypt the request and send it to the base station. The base station sends the K_n by encrypting it by K_o of particular node. Only the node which is authenticated can decrypt the message and get Kn. Thus, this key is used for BS:N, as well as N:CH communications.

Data Transmission Phase

After clustering is completed and each node gets its keys in key establishment phase, then it is the time to start data transmission phase. This phase begins from intra-clustering communication and end with inter-clustering communication as follows:

- *Intra-clustering communication:* An ordinary node can initiate a message (M) at first and forwards it to DCH:

$$M = \{ K_b\ ,\ Ts\ ,\ MAC \} \quad (3)$$

where, K_b is a buddy key with DCH, *Ts* is the time stamp for avoiding replay of the message, and MAC is the

message authentication code. DCH and RCH communicate with each other by using the buddy key between them. They are already having 'buddy info table', and they are members in the cluster:

$$DCH\ (DM) = \{K_{b1}\ (K_b, Ts, MAC, aggregated\ (M))\} \quad (4)$$

where, K_{b1} is the buddy key between DCH and RCH. In a situation when the number of nodes in a sector is small, the RCH can play the RCH and DCH role at the same time to save energy.

- *Inter-clustering communication:* Now the message must route to the base station directly and the node that represents the routing cluster head must switch on to the long radio communication. In this stage the broadcast key (K_c) is needed to encrypt the message. To get the broadcast key, CH members use their own-key and request the key from the base station. The routed message will become:

$$RCH\ (RM) = \{K_c\ \{K_{b1}\ \{K_b, Ts, MAC, (DM)\}\}\} \quad (5)$$

ADDING AND DELETING NODES

When a node loses its battery power, compromised, or is completely dead by any reason, we assume that the node has been deleted. The deleted information is updated to all the nodes within the cluster. If the deleted node is cluster head then new head node must be selected by the base station using the parameters mentioned previously.

When nodes are added to network, the new nodes must register at the base station. Then based on their locations, they will join the suitable clusters. If an added node is not within the range of any cluster, then that node will form a new cluster with no other members in it. This node will switch to long rang radio communication to participate in communication with others members. At any moment this node joins any cluster, it will turn off its long rang radio to reduce the power consumption.

ADAPTATION TO MOBILITY

Our scheme is proposed for moderate movement WSNs. We assume that the base station and all sensor nodes have the ability of such movement. However, we also assume that the zone in which the base station moves is known a priori. Two important things constitute to the system capability for adaption to mobility. The first is a direct result from the adopted mobility model. According to this model, the location of the base station at certain time is predictable with certain probability. Indeed, the location of any sensor at any certain time can also be predictable with a certain probability.

Secondly, due to the assumed GPS free solution, the base station can discover the changes in the relative sensor locations due to mobility by periodically updating such information each certain period of time. As mentioned previously, this time interval can be specified by the base station depending on the mobility level of the nodes. Thus, it is an important design parameter that should be chosen carefully. A longer time interval will cause the scheme less adaptable to mobility effects, while shorter periods might unnecessarily increase communications and computation loads. This latter case causes the base station to initiate reforming the clusters more frequently than what is actually required to track the network mobility effects. This would result in a fast consumption of energy of nodes, i.e. decreasing the life time of sensor nodes.

SECURITY ANALYSIS

In this paper, we have proposed a new key management scheme for mobile WSNs. The security of the proposed key management scheme comes from the way of using various secret keys for different communication types. Keys like broadcast key and network key are distributed by the base station, while keys like buddy key and own key are calculated by each node through using pre-deployed unique id and other information that represents the changing environment with respect to track-sector logical context. In our scheme, the base station afforded most of the work load and computation in order to avoid these activities in the sensor nodes which are limited in energy power, memory size, and processing computation.

The formation of clustering using tracks and sectors reduces redundant data transmission in the network by breaking the long links in to smaller links. Also reduces the distance for transmission of data from the nodes to their cluster head which means one-hop between the nodes and cluster head in each cluster in the network.

As stated in [19], using a single technique is not perfect to secure all the communication in the sensor networks. Therefore a good strategy is using combination of different keying techniques like 'in-network generated keys', 'pre-deployed keys', and 'broadcast keys'. After 'neighbour discovery' phase overall, the nodes build their 'buddy info table' and the base station initiates the key distribution process.

It's possible that an attacker can capture some nodes in the network. Since sensor nodes are generally not tamper-proof, an attacker can access to the key table in the captured nodes. An attacker can put capture nodes in the network again; he/she then can decrypt messages sent to and from the captured nodes. Thus in the worst case an, attacker can compromise all the nodes that belongs only to one buddy set and not all network. So, the survivability of the network cannot be easily degraded significantly.

Key refreshment in this scheme are declared in the updating of broadcast key and network key at regular intervals of time by the base station. This refreshment proves the authentication for the nodes that belonging to the network from time to time. The key maintenance of each node in the network maintains a database for the following keys: its own key, its buddy key, network key, and broadcast key for CH nodes only. Finally, our scheme restricts the number of the neighbours because of the division of the network into tracks and sectors. This significantly affects the number of key establishments needs to be done. Therefore, any attack on any cluster does not compromise the whole network. This also has another benefit which is saving the energy in each node.

CONCLUSION

In this paper, we have presented the use of track-sector hierarchical clustering in mobility environment in order to achieve key management. The proposed scheme is based on symmetric key cryptographic because it does not heavy computations as their public-key peers. Our scheme combines more than one technique and mechanism of key management. It also takes into account the issue of energy consumption. The scheme is proposed for moderate movement environments. As our work is still in progress, more details about our implementation and the obtained experimental results will be presented by a subsequent paper.

REFERENCES

[1] Zhang, J. and Varadharajan, V. (2010). Wireless sensor network key management survey and taxonomy. *Journal of Network and Computer Applications,* 33**,** 63-75.

[2] Zhou, Y., Fang, Y. and Zhang, Y. (2008). Securing Wireless Sensor Networks: A Survey. *IEEE Communications Surveys & Tutorials,* 10**,** 6-28.

[3] Yang, H., Luo, H. Y., Ye, F., Lu, S. W. and Zhang, L. (2004). Security in Mobile Ad hoc Networks: Challenges and Solutions. *IEEE Wireless Communications,* Vol. 11**,** pp. 38-47.

[4] Sarma, H. K., Kar, A. and Mall, R. (2009). Energy Efficient Communication Protocol for Mobile Wireless Sensor Network System. *IJCSNS,* Vol. 9**,** pp.386-394.

[5] Gautan, N., Lee, W. and Pyun, J. (2009). Track-sector Clustering for Energy Efficient Routing in Wireless Sensor Network. *The 9th IEEE International Conference on Computer and Information Technology,* Vol. 2**,** pp. 116-121.

[6] Eschenauer, L. and Gligor, D. (2002). A key management scheme for distributed sensor networks. *The 9th ACM Conference on Computer and Communications Security,* Washington DC , USA.

[7] Chan, H., Perrig, A. and Song, D. (2003). Random Key Predistribution Schemes for Sensor Networks. *IEEE Symposium on Research in Security and Privacy* Oakland, California USA.

[8] Liu, D., Ning, P. and Du, W. (2005). Group-Based Key Pre-Distribution in Wireless Sensor Networks. *Proceedings of 2005 ACM Workshop on Wireless Security (WiSe 2005).*

[9] Shen, L., Feng, H., Qiu, Y. and Ding, H. (2008). A New Kind of Cluster-based Key Management Protocol in Wireless Sensor Network. *Proceedings of the IEEE Conference of Networking, Sensing and Control.*

[10] Deng, J., Han, Y., Chen, S. and Varshney, P. (2004). A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge. *IEEE INFOCOM 2004.* Los Alamitos, CA , USA.

[11] Liu, D. and Ning, P. (2003). Location-based pairwise key establishments for static sensor networks. *First ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'03),* New York, NY, USA

[12] Yu, Z. and Guan, Y. (2008). A key management scheme using deployment knowledge for wireless sensor networks. *IEEE Transactions on Parallel Distribution and Systems,* 19**,** 1411–1425.

[13] Huang, D., Mehta, M., Medhi, D. and Harn, L. (2004). Location-aware key management scheme for wireless sensor networks. *The 2nd ACM workshop on Security of Ad Hoc and Sensor Networks.*

[14] Kifayat, K., Merabti, M., Shi, Q. and Llewellyn-Jones, D. (2010). Group-based key management for mobile sensor networks. *Proceedings of 2010 IEEE Sarnoff Symposium.* Princeton, NJ, USA.

[15] Zhou, Y., Ni, J. and Ravishankar, C. (2005). Efficient Key Establishment for Group-Based Wireless Sensor Deployments. *Proceedings of the 4th ACM Workshop on Wireless Security (WiSe '05),* Cologne, Germany, September, 2005.

[16] Ünlü, A. and Levi, A. (2010). Two-tier, scalable and highly resilient key predistribution scheme for location-aware wireless sensor network deployments. *Mob. Netw. Appl.,* Vol. 15, No. 4**,** pp. 517-529.

[17] Dong, Q. and Liu, D. (2007). Using auxiliary sensors for pair-wise key establishment in WSN. *Proceedings of the 6th international IFIPTC6 Conference on Ad Hoc and Sensor Networks, Wireless Networks, Next Generation internet,* Atlanta, GA, USA, May 14 - 18, 2007.

[18] Sensoria (2012). Sensoria. *Sensoris Corporation* [Online]. Available on: www.sensoria.com.

[19] Sharma, K., Ghost, S.K. and Ghost, M.K. (2009). Security Model For Hierarchical Clustered Wireless Sensor Network. *International Journal of Computer Science and Security.*

أسلوب لإدارة مفاتيح التشفير في شبكات المتحسسات اللاسلكية المتنقلة

فؤاد سليم مبارك سفيان تايه فرج

fualku1968@yahoo.com

الخلاصة:

إن شبكات المتحسسات اللاسلكية هي عبارة عن شبكات محدودة المصادر من غير هيكلية محددة ، وهي تتألف أساسا من عدد كبيرمن عقد التحسس. وتقوم عقد التحسس هذه بجمع المعلومات من المنطقة المشمولة ومن ثم إيصالها إلى المحطة الرئيسية. وهذه الشبكات عادة ما يتم نشرها في مناطق مفتوحة لذلك فهي بحاجة ماسة إلى تقنيات أمنية للحماية. ولغرض حماية أمن معلومات هذه الشبكات فلابد أولا من وضع أسلوب أمين وقوي لأدارة مفاتيح التشفير فيها. هذا وقد تم دراسة مشكلة إدارة مفاتيح التشفير بشكل جيد في شبكات المتحسسات اللاسلكية الاعتيادية (الثابتة)، لكن هذه المشكلة في شبكات المتحسسات اللاسلكية المتنقلة لازالت بحاجة الى دراسات أعمق. ويعود هذا إلى أنه عند ادخال قابلية التنقل إلى شبكات المتحسسات اللاسلكية فسوف تظهر عدة تحديات وخواص جديدة ينبغي أخذها في نظر الاعتبار في النموذج الأمني. إن المتطلبات الأمنية الأساسية التي ينبغي تحقيقها في هذه الشبكات تتضمن الوثوقية والسرية والسلامة، وتعد إدارة المفاتيح حجر الزاوية في تحقيق هذه المتطلبات. وفي هذا البحث يتم اقتراح أسلوب جديد لإدارة مفاتيح التشفير في شبكات المتحسسات اللاسلكية المتنقلة ، حيث يعتمد الاسلوب المقترح على تقسيمات المسار–القطاع ضمن نطاق التنقل. وقد تم بناء المقترح على أساس التشفير المتناظر لتحقيق الأهداف المرجوة. ونقوم في هذا البحث برصد تقدم العمل البحثي في تطوير وتنفيذ أسلوب توزيع وإدارة مفاتيح التشفير المقترح.