RESEARCH ARTICLE OPEN ACCESS

MASDKM: Mobile Agent Based Secure and Dynamic Key Management Scheme for Wireless Sensor Networks

Ramu Kuchipudi [1], Dr. Ahmed Abdul Moiz Qyser [2], Dr. V V S S S Balaram [3]
Department of CSE [1]
Vardhaman College of Engineering, Shamshabad
Department of CSE [2]
Muffakham Jah College of Engineering
Department of IT [3]
Sreenidhi Institute of Science & Technology
Hyderabad, India

ABSTRACT

Secure key management is fundamental need in WSN to safeguard sensitive communications. One of the attractive solutions in WSN is symmetric key cryptography which is relatively faster and energy efficient. However, it cannot bestow high level of security due to difficulty in secure key management. Nevertheless, Asymmetric key cryptography can enhance network security but it also causes energy, memory and computational overhead. In this paper we proposed Mobile Agent Based Secure and Dynamic Key Management Scheme (MASDKM). This scheme has two levels that exploit good features of asymmetric and symmetric cryptography respectively. In the first level we introduced agent based key distribution and coordination for asymmetric keys while the second level is sensor nodes can involve in constructing symmetric keys for secure communication through mutual authentication and encryption with those keys. Agent based public key dissemination and update of shared keys could reduce communication overhead. We evaluated the system using NS3 simulations. The results reveal that the performance of the proposed scheme is significantly better when compared with its asymmetric counterparts.

Keywords **:-** Wireless Sensor Network (WSN), security, key management, mobile agent, key distribution**.**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) became ubiquitous technologies for building future networks. They are used in civilian and military applications where nodes capture and send sensitive data to base station. Moreover the nodes in WSN are resource and vulnerable to attacks. Therefore protecting such networks using cryptographic primitives is inevitable. The widely accepted solution to this problem is exchanging signed messages with private or public key cryptography. Public key cryptography can enhance security of WSN. However, it causes more overhead in terms of memory, and computation. On the other hand private key cryptography has problem with key management. However, the private key cryptography is relatively faster and energy efficient.

II. RELATED WORK

In WSN key distribution is a challenging phenomenon for many reasons such as constrained resources like memory, energy, transmission range, and processing power. The key distribution mechanisms found in the literature can be categorized into static and dynamic key management schemes. As the name implies, the static key management schemes stores all keys in sensor nodes. Each sensor node can obtain shared keys from its neighbours. A sensor node is capable of setting up a shared key using intermediate nodes. The static keys when compromised, the security of network is lost. In case of dynamic key management session keys are established using the preloaded keys in the sensor nodes. Here keys are changed dynamically and for adversaries it is not easy to break security. The key management architectures are also of two types. They are asymmetric and symmetric architectures.

Gu *et al.* [1] explored the scalability of key pre-distribution protocols in WSN. Especially they defined a new metric known as Resilient Connectivity (RC) to measure the security performance of key pre-distribution (KP) protocols in WSN. They focused on the scalability of security performance rather than computation and communication overhead. From their research they could formulate two scaling laws for KP protocols. First, with respect to RC the KP protocols are scalable as far as node density is considered. Second, with respect to RC the KP protocols are not scalable as far as network dimension is considered. Rasheed *et al.* [6] proposed two KP schemes which help mobile sink to establish secure communication with any sensor node in the network. Their schemes are based on three things such as Q-composite [15], probabilistic generation KP [16], and polynomial pool based KP [17]. It is resilient against node capture attacks. Later on Rasheed *et al*. [8] improved the authentication mechanism and prevented replication attacks. Khan *et al*. [7] proposed a KP scheme for WSN which is memory efficient and matrix-based. The scheme provides high scalability and network connectivity. It has provision for a link key so that the existing nodes' information is intact when new nodes are added.

Another KP scheme was proposed by Bechkit *et al*. [9] for high level of scalability and network connectivity. The scheme made use of enhanced unital-based approach with less storage overhead. Ruj *et al*. [2] proposed a mechanism for addressing pair-wise and triple key establishment issues in WSN. In this approach three nodes are able to share a common key. Their approach was based on combinatorial and polynomial for triple key distribution. The proposed pair-wise and triple key establishment is used to have secure data aggregation in WSN. Then the scheme was applied to key management and secure forwarding in WSN. It was proved to be resilient against node capture attacks. The advantage of the scheme is that it can be applied to both static and dynamic networks with clustering. However, the security of this scheme is limited by the use of degree of polynomials.

Most recently Seo *et al*. [3] focused on dynamic key management in dynamic WSN. They proposed a protocol known as Certificate less-effective key management (CL-EKM). This scheme provides secure communications in WSN besides having ability to support backward and forward secrecy. The protocol has mechanisms to update keys when a new node joins the network or an existing node leaves the network. It can also detect compromised nodes and performs key revocation effectively. When a node is compromised, it minimizes the impact on other nodes in the network. It is robust against many attacks such as impersonation, cloning, and node compromise. Klaoudatou *et al*. [4] made a good review of cluster-based protocols especially for group key management in WSN. Gandino *et al*. [14] proposed an innovative key management scheme for secure communications. The scheme was named as random seed distribution with transitory master key. The secret material is randomly distributed and to generate pairwise keys transitory master key is used to provide high level of security.

Alagheband and Aref [5] proposed a dynamic key management scheme for WSN based on Elliptic Curve Cryptography (ECC). They used heterogeneous network and signcryption method as part of the key management scheme. Sensor node mobility and network scalability are important features of the network considered. A new registration mechanism and periodic authentication were implemented to avoid SN compromise. The scheme is known for its improved key storage, computation, and communication. Ya-nan *et al*. [10] proposed a scheme for intra-cluster key sharing for secure communication in a hierarchical WSN. It could reduce storage and communication overheads besides achieving 100% connectivity as far as intra-cluster communication is concerned. Yagan *et al*. [11] explored pairwise KP scheme in WSN in the presence of unreliable links. Zhou *et al*. [12] focused on heterogeneous sensor networks (HSNs) which are static in nature for continuous secure scheme. Two dimensional backwards chains are used to achieve the continuous secure scheme. The probability of compromising shared keys is reduced and continuous secure aspect is improved significantly. Yagan *et al*. [13] studied on the connectivity of WSN in the presence of random pairwise KP and found the high probability of network connectivity.

Our work is close to the work of Sahingoz [18] who proposed multi-level dynamic key management scheme for WSN where UAV is the mobile certification authority used to distribute public keys. In this paper we proposed scheme that makes use of mobile agents instead of UAV for public key distribution. Our scheme reduces communication overhead, memory overhead and computational overhead. Besides, it is resilient against node capture attacks.

III. SYSTEM ARCHITECTURE OF MASDKM

We proposed an agent based system architecture which is aimed at dynamic key management in dynamic WSN. The architecture is named as Mobile Agent Based Secure and Dynamic Key Management Scheme (MASDKM). It has two layers broadly. They are dynamic key management and mobile agent manager. The dynamic key management involves key distribution, key update, join or leave and key agreement protocol. The mobile agent manager layer takes care of mobile agents and other activities such as communication, coordination, resource management and data management with respect to the mobile agents. The MAM manages two mobile agents namely key distribution agent (KDA) and location calculation agent (LCA).

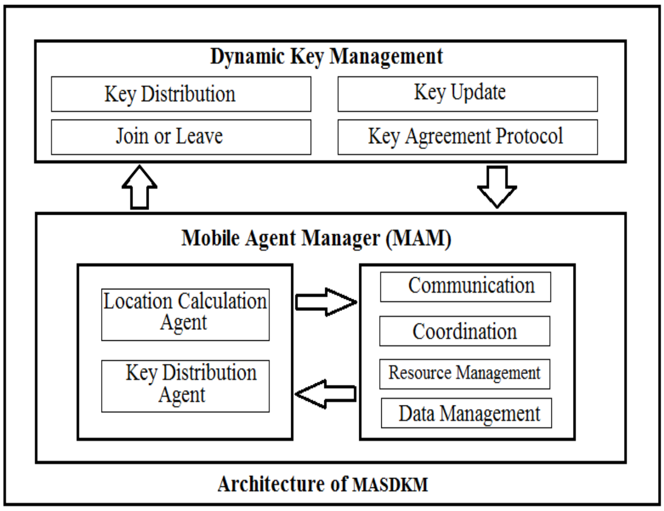

Fig.1 – Overview of proposed system architecture of MASDKM

As shown in Figure 1, mobile agent manager controls the movement of mobile agents in the WSN. LCA is responsible for finding the location of sensor nodes, CHs and BS. The location information is used by the KDA which is responsible to provide public keys to sensor nodes in order to have a dynamic and secure key establishment.

IV. NETWORK MODEL FOR MASDKM

The proposed WSN is made up of three kinds of devices namely sensor node (SN), cluster head (CH) and base station or sink (BS). SN is a node that has limited resources such as memory, processing power, battery power and transmission range. SN is responsible to send data and send it to its cluster head. Cluster is a collection of logically grouped sensor nodes. The CH possesses more resources when compared with SN. Aforementioned resources including transmission range is high with CH. CH can communicate with its member SNs and also base station. CH is responsible to collect data from SNs of the cluster and aggregate it before sending to BS.

The concept of clusters can increase the lifetime of network. BS is a node in the WSN which is not resource constrained.

Virtually it has unlimited resources. It has very high transmission range to reach every node in the network. BS is a device which is well-protected. This kind of WSN is widely used as the cluster based approach to optimize resource utilization. However, we employ the concept of mobile agents for secure key establishment. Our network model consists of four important components such as BS, CH, SN, and Mobile Agent Manager (MAM).

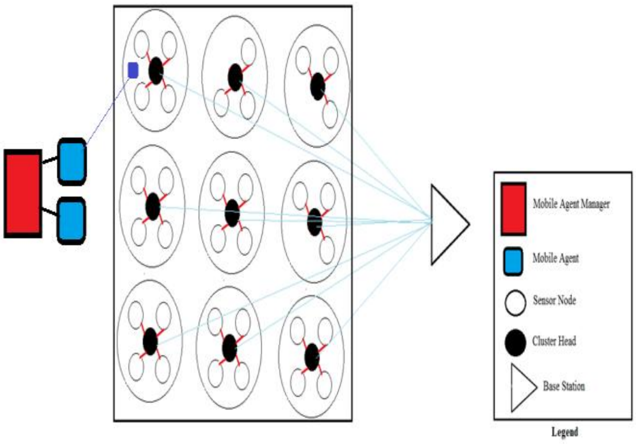

Fig. 2 Proposed network model

As shown in Figure 2, the network model has many components such as base station, sensor node, cluster head, mobile agent and mobile agent manager.

A. *Sensor Node (SN)*

SN is the core component of WSN whose purpose is to sense data and sends to CH in either a single or multi-hop path. It is an inexpensive electronic device with limited resources such as storage, energy, transmission range, and processing capability.

B. *Cluster Head (CH)*

The concept of clustering and each cluster having a selected CH improve network lifetime. The rationale behind this is the systematic approach in data aggregation and dissemination. In fact CH is also a sensor node but with more responsibilities. Obviously it is a node with more resources especially energy, memory and long transmission range. The objective of CH is to collect data from nodes in the cluster, aggregate it and send it to BS.

C. *Base Station (BS)*

It is very significant component in WSN as it collects data in WSN and sends to the managers who know the utility of such data. It sends data to managers through Internet. It also manages WSN. It is well protected and ensured that it is not limited by power and other resources. It runs round the clock and provides necessary information to intended audience.

D. *Mobile Agent Manager (MAM)*

This component is crucial for distribution of public keys to sensor nodes in WSN. This is the component which makes use of mobile agent to achieve the task. Stated differently MAM distributes public keys to SNs through mobile agent.

E. *Mobile Agent*

It is a software component which is self contained. It is a program which can migrate from its host to other nodes in WSN and provide public keys. Once it is initiated by MAM, it becomes independent of MAM and performs its duty without human intervention. This program when executed at a node can suspend its execution and move on to next node as required.

F. *Threat Model*

Generally WSN is deployed in hostile environments and the communicating nodes cannot be trusted in general. The communication channel is assumed to be insecure. The nodes in the network are vulnerable and the security keys can be stolen by adversaries. The attacks launched on such network are categorized into passive and active attacks. Passive attacks are limited to the eavesdropping messages without disrupting the communication process. The active attacks on the other hand may inject packets into the network, interrupt normal communication besides eavesdropping. If attacker can gain access to secret keys, he can use a compatible device and community with other devices by injecting false data. Such attacks are known as insider attacks. Outsider attacks on the other hand are launched without known secret keys from outside the network.

G. *Key Distribution*

The proposed key management scheme is dynamic and hybrid in nature. For this reason, only private key is stored in sensor node. The sensor node also holds the public key of mobile agent (MA). Once deployment is over secure communications between two users is done as follows. To achieve this, a node needs to know the ID of other node. A sender node gets IDs of other nodes and executes the proposed key distribution algorithm. Figure 3 illustrates the operations involved in secure key distribution.

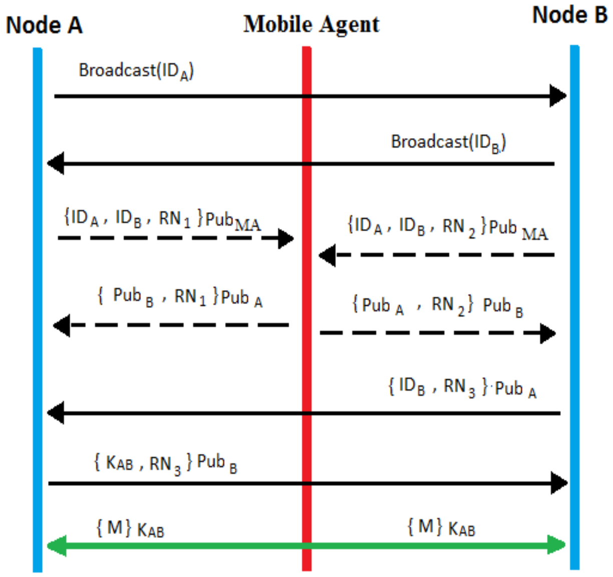
Node A
Mobile Agent
Node B
Broadcast(ID$_A$)
Broadcast(ID$_B$)
{ID$_A$, ID$_B$, RN$_1$ }Pub$_{MA}$
{ID$_A$, ID$_B$, RN$_2$ }Pub $_{MA}$
{ Pub $_B$, RN$_1$ }Pub $_A$
{ Pub $_A$, RN$_2$} Pub $_B$
{ ID$_B$, RN$_3$ } Pub $_A$
{ K$_{AB}$, RN$_3$ } Pub $_B$
{ M } K$_{AB}$
{ M } K$_{AB}$

Fig. 3 Secure key distribution model

The node A and node B are SNs in the WSN. Mobile agent is the autonomous program that is meant for distributing public keys to SNs. Finally the communication pariwise key K_{AB} is securely established between A and B. More details of the mechanism are described in the proposed key agreement protocol.

V. PROPOSED KEY AGREEMENT PROTOCOL

A sensor node can establish shared key with one of its neighbour node as per the key agreement protocol described here.

Key Agreement Protocol

- Each sensor node in the WSN broadcasts a message containing its ID to all its neighbouring nodes
- Then the neighbouring nodes (B and others) obtain public key of A from the Mobile Agent known as Key Distribution Agent (KDA). The request for other nodes' public key is sent to KDA by encrypting message with public key of KDA.
- On receiving public key request from A, the MAM initiates KDA. KDA takes the location of A from LCA and moves to the node A returns the requested key by encrypting it with public key of A.
- Then node B does the following
    a. Uses public key of A to encrypt message
    b. The message also contains ID of node B denoted as ID_B and a random number (RN_1)
    c. RN_1 is used to identify the transaction and to get rid of replay attacks
- Afterwards, node A does the following
    d. Decrypts the message received
    e. Obtains random number of ID of neighbour node
    f. Selects a secret key denoted as K_{AB} and RN_1
    g. Encrypts them with public key of B denoted as Pub_B
    h. Send it to B
- Thus verifying both communicating parties has been completed and the encrypted messaging ensures satisfactory level of security.

A. *Adding New Nodes*

Since it is a dynamic WSN new nodes can be added and existing nodes can leave the network. These events are supported in the proposed scheme for scalable network. The newly joined nodes in the network are able to establish shared secrets with its neighbours.

B. Key Update

Shared keys once established can be used for secure communications. However, keeping them intact for long time is not a good approach as it can result in attacks. Every key is associated with a life time. Once it is expired it is necessary to perform key update. This will enable WSN to have network survivability to get improved and compromised nodes' keys are updated to avoid security risks further. The key update is done based on the time elapsed based on a threshold and also based on the volume of data traffic. In case of traffic, when traffic reaches the threshold, key update is taken place automatically. For the purpose of key update, there is no need to contact MAM. The reason behind this is that nodes have the public keys of neighbours. When a node wants to update shared key between it and its neighbour it sends such request to its neighbour.

The key distribution mechanism proposed in this paper can improve the efficiency of network in different dimensions.

- It reduces the memory usage. The nodes in the network hold public keys of neighbours and shared keys established with them. Therefore the storage cost is not dependent on the number of nodes that are in the WSN. This significantly improves scalability.
- In the key distribution and key update phases, it reduces communication overhead. Once public key is obtained from the KDA, it does not need to communicate with MAM again. The nodes under communication can set up shared keys. No additional message traffic is produced. Thus the total amount of traffic is reduced.
- The communication cost in the sensor node is reduced. This is due to the use of symmetric keys for internal communication which is faster. Only in case of setting up shared keys, it makes use of public key encryption which is generally costly.
- It promotes network life time due to the reduction in power consumption, reduction in communication overhead and reduction in memory usage.
- It promotes extendibility as it does not need additional memory for accommodating new nodes in the network.

C. Location Calculation

This is the mechanism used by LCA which is employed by MAM. The procedure assumes the whole WSN to have virtual grids. Each node's location is denoted as (x,y) while the location of CH is denoted as (X,Y). The coverage area of CH is denoted as L.

For a sensor node positioned at (x,y)
Home grid is computed as (X,Y) with
$X = x/L$
$Y = y/L$
There grid centre is (X_0, Y_0) where
$X_0 = (X+1/2)L$
$Y_0 = (Y+1/2)L$

VI. PERFORMANCE EVALUATION

The proposed architecture and network model with underlying dynamic key management based on mobile agents are evaluated in terms of communication overhead, memory usage and resilience against node capture attacks.

A. Memory Usage

For secure and scalable communications, each SN needs to store public keys and shared keys of only its neighbours. Therefore the memory usage does not increase when number of nodes in the network is increased.

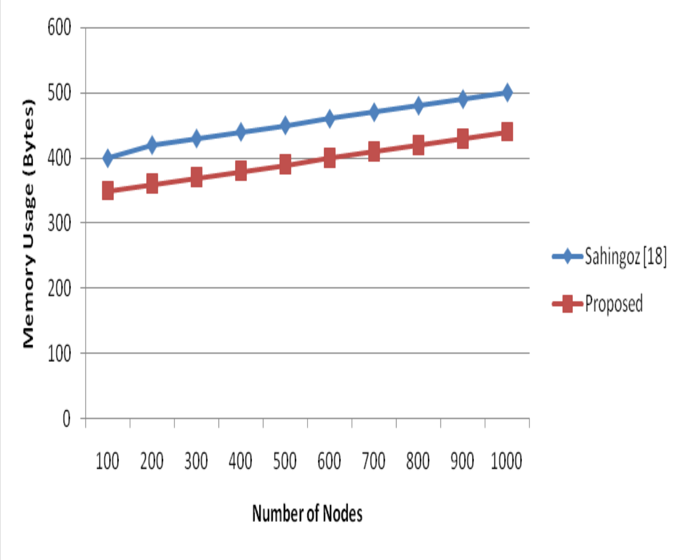

Fig. 4 Memory usage performance

As shown in Fig 4, it is evident that horizontal axis represents number of nodes while the memory usage is represented by vertical axis. The results revealed that the proposed system has performance improvement over that of [18] with respect to memory usage.

B. Resilience against Node Capture

The proposed system there is unique shared key between any two communicating nodes in WSN. If any SN is captured, it only affects its neighbours instead of affecting the whole network.

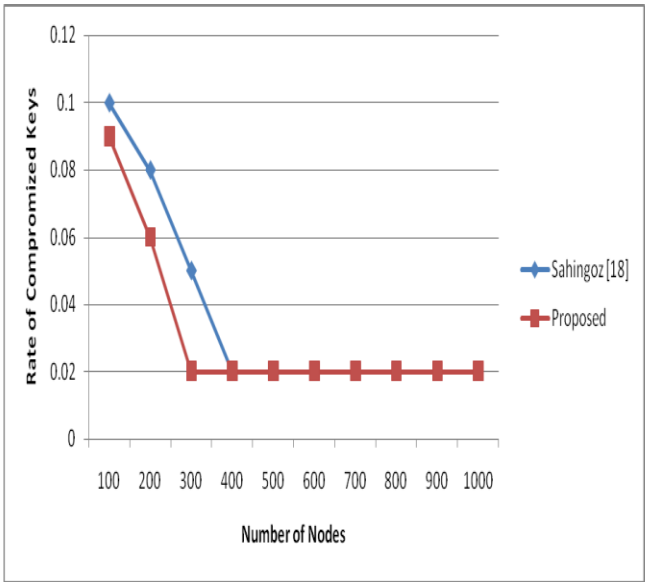

Fig. 5 Resilience against node capture

As shown in Fig 5, it is evident that horizontal axis represents number of nodes while the rate of compromised keys is represented by vertical axis. The results revealed that the proposed system has performance improvement over that of [18] with respect to compromised keys.

C. *Communication Overhead*

In the network initialization phase, the sensor nodes obtain public keys from the KDA. Then each node establishes shared secret key with its neighbours. It results in the communication overhead while setting up shared session key.

VII. CONCLUSION AND FUTURE WORK

In this paper we proposed Mobile Agent Based Secure and Dynamic Key Management Scheme (MASDKM). It exploits benefits of multi-level dynamic key management and the mobile agent based key distribution. The dynamic key management is realized by using both symmetric and asymmetric cryptography. In the first level we introduced agent based key distribution and coordination for asymmetric keys while the second level is sensor nodes can involve in constructing symmetric keys for secure communication through mutual authentication and encryption with those keys. Agent based public key dissemination and update of shared keys could reduce communication overhead. The MAM is the proposed system architecture is responsible to provide two kinds of agents such as LCA and KDA. The LCA computes the location of nodes in WSN while the KDA provides public keys to nodes in WSN. The proposed system is evaluated with memory consumption, communication overhead, and resilience against node capture attack. The empirical results revealed that the proposed system has significant performance improvement over existing systems. This research can be extended further by improving the scheme and validate it with other possible attacks.

REFERENCES

[1] Wenjun Gu, Sriram Chellappan, Xiaole Bai, and Honggang Wang. (2011). Scaling Laws of Key Predistribution Protocols in Wireless Sensor Networks. *IEEE*. 6 (4), p.20-30.

[2] Sushmita Ruj, Amiya Nayak and Ivan Stojmenovic. (2013). Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications. *IEEE*. 62 (11), p.45-56.

[3] Seung-Hyun Seo, Jongho Won, Salmin Sultana and Elisa Bertino. (2015). Effective Key Management in Dynamic Wireless Sensor Networks.*IEEE*. 10 (2), p.90-101.

[4] Eleni Klaoudatou, Elisavet Konstantinou, Georgios Kambourakis, and Stefanos Gritzalis. (2011). A Survey on Cluster-Based Group Key Agreement Protocols for WSNs. *IEEE*. 13 (3), p.12-19.

[5] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, “A novel ultrathin elevated channel low-temperature poly-Si TFT,” *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[6] Amar Rasheed and Rabi N. Mahapatra. (2011). Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks. *IEEE*. 22 (1), p.12-19.

[7] E. Khan E. Gabidulin2 B. Honary H. Ahmed. (2011). Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks. *IET Wirel. Sens*. 2 (2), p.90-101.

[8] Amar Rasheed and Rabi N. Mahapatra. (2012). The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks. *IEEE*. 23 (5), p.80-86.

[9] Walid Bechkit, Yacine Challal, Abdelmadjid Bouabdallah, and Vahid Tarokh. (2013). A Highly Scalable Key Pre-Distribution Scheme for Wireless Sensor Networks. *IEEE*. 12 (2), p.12-19.

[10] Liu Ya-nan, Wang Jian, Du He, Sha Li-jun. (2013). Intra-cluster key sharing in hierarchical sensor networks. *ISSN*. 3 (3), p.90-101.

[11] Osman Yağan and Armand M. Makowski,. (2013). Modeling the Pairwise Key Predistribution Scheme in the Presence of Unreliable Links. *IEEE*. 59 (3), p.45-56.

[12] Boqing Zhou, Jianxin Wang, Sujun Li, Yun Cheng, and Jie Wu. (2013). A Continuous Secure Scheme in Static Heterogeneous Sensor Networks. *IEEE*. 17 (9), p.90-101.

[13] Osman Yağan and Armand M. Makowski. (2013). On the Connectivity of Sensor Networks Under Random Pairwise Key Predistribution. *IEEE*. 59 (9), p.20-30.

[14] Filippo Gandino, Bartolomeo Montrucchio and Maurizio Rebaudengo. (2014). Key Management for Static Wireless Sensor Networks With Node Adding.*IEEE*. 10 (2), p.80-86.

[15] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution Schemes for Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2003.

[16] S. Hussain, F. Kausar, and A. Massod, "An Efficient Key Distribution Scheme for Heterogeneous Sensor Networks," Proc. Int'l Conf. Wireless Comm. and Mobile Computing (IWCMC), 2007.

[17] D. Liu, P. Ning, and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks," Proc. 10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 52-61, Oct. 2003.

[18] Ozgur Koray Sahingoz. (2013). Large scale wireless sensor networks with multi-level dynamic key management scheme. *Elsevier*, p.20-30.