Advances in Wireless and Mobile Communications.
ISSN 0973-6972 Volume 10, Number 1 (2017), pp. 65-78
© Research India Publications
http://www.ripublication.com

Mobile Agent Based Key Distribution Approach for Clustered Wireless Sensor Networks

Ramu Kuchipudi[1] , Dr. Ahmed Abdul Moiz Qyser [2], Dr. V.V.S.S.S. Balaram [3]

[1]Associate Professor , Department of CSE [1]
Vardhaman College of Engineering, Shamshabad, Telangana, India.

[2]Professor and Head, Department of CSE [2]
Muffakham Jah College of Engineering, Banjara Hills, Telangana, India.

[3]Professor and Head, Department of IT [3]
Sreenidhi Institute of Science & Technology, Yamnampet, Telangana, India.

Abstract

Key management is very crucial need in WSN to protect data and secure communications. One of the Key distribution 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 Dynamic Key Management Scheme. 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 NS2 simulations. The results reveal that the performance of the proposed scheme is significantly better in terms of communication, memory, and computation overheads when compared with its asymmetric counterparts.

I. INTRODUCTION

Wireless Sensor Network is a collection of sensor nodes that are used to capture information from surroundings. When Wireless Sensor Networks are deployed in a hostile environment security becomes extremely important. An Opponent can eavesdrop of secret information. An adversary can provide misleading information to other nodes. Therefore sensor devices are vulnerable to different kinds of attacks. Preventing attacks in WSN is to be given highest importance. The open problem in Wireless Sensor Networks is How to set up secret keys between communicating nodes?.

There are three types of Key distribution schemes. They are Trusted server or Arbitrated schemes, Self-enforcing schemes and Key-Predistribution schemes. Trusted server schemes depend on trusted server for key distribution between nodes. Kerberos is an example for Trusted server scheme. Trusted server scheme is not suitable for Wireless Sensor Networks because there is no trusted infrastructure in sensor networks. Self enforcing schemes depend on Public key cryptography to distribute keys using public key certificates. It is not very convenient to use due to limited resources of sensor nodes.

In the Key-predistribution scheme key information is distributed among all sensor nodes prior to deployment. Before deployment of sensor network nodes are loaded with keys using key distribution center. A Key predistribution scheme has three phases. They are key distribution phase, shared key discovery and path key establishment phase. Key predistribution is also divided into probabilistic and deterministic schemes based on existence of the shared keys.The main problem in this scheme is every node has to store more number of keys.

Key distribution schemes are classified into static and dynamic catagories based on whether update of master keys or administrative keys. Both administrative and communication keys need to be changed to thwart security attacks. Network survivability and Scalability are the advantages of Dynamic key management. The major difficulty in dynamic key management is efficient rekeying.

Dynamic key management in dynamic WSN is a challenging problem to be addressed. The existing approaches focuses on different means of key distribution in WSN. Recently Sahingoz [1] proposed a multi-level dynamic key management scheme for large scale WSN. Their scheme makes use of both symmetric and asymmetric cryptographic primitives to have the synergic effects of both while reducing overhead on WSN. However, usage of mobile agents for key distribution in WSN is the research area little explored.

The remainder of the paper is structured as follows. Section II provides review of literature. Section III presents the proposed system in detail. Section IV presents implementation details. Section V shows experimental results while section VI concludes the paper.

II. RELATED WORK

Key management can be defined as a set of processes and mechanisms that support key establishment and the maintenance of ongoing keying relationships between valid parties according to a security policy.

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.

Rasheed *et al.* [6] proposed two KP schemes which help mobile sink to establish secure communication with any sensor node in the network. 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.

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.

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.

Klaoudatou *et al.* [4] made a good review of cluster-based protocols especially for group key management in WSN. Alagheband and Aref [5] proposed a dynamic key management scheme for WSN based on Elliptic Curve Cryptography (ECC). 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.

This paper is close to the work of Sahingoz [1] 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. PROPOSED SOLUTION

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 1 illustrates the operations involved in secure key distribution.

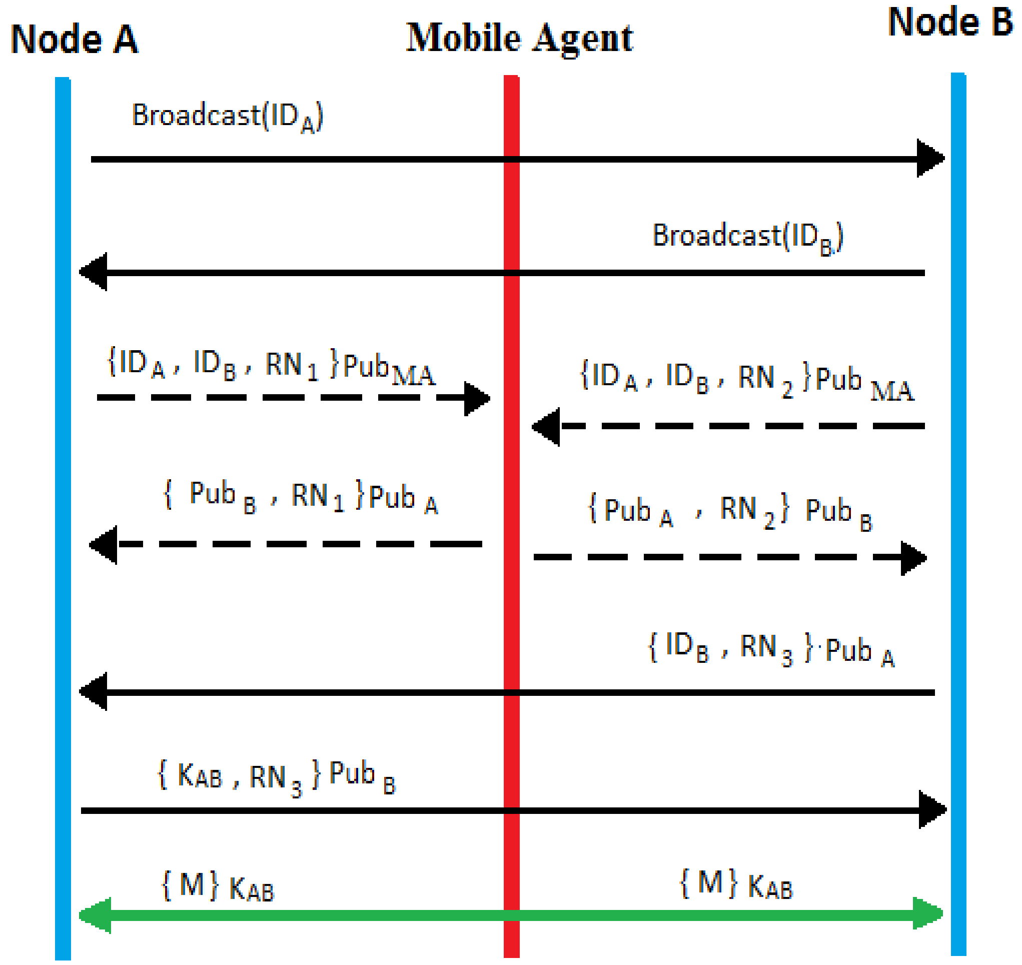

Figure 1. Secure key distribution model

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 pair wise key K_{AB} is securely established between A and B. More details of the mechanism are described in the proposed key agreement protocol.

As shown in Fig 2, it is evident that the network has many things associated. They are known as Mobile Agent Manager (MAM), Mobile Agent (MA), Sensor Node (sn), Cluster Head and Base Station. The MAM can be considered a class of mobile agents. It can produce a mobile agent on demand. Then the mobile agent will start doing its intended functionality in cost effective fashion besides being autonomous from its producer. Thus it is possible to have multiple instances of mobile agents if required. We assume that one mobile agent instance is sufficient in the proposed model which has limited number of sensor nodes. The mobile agent is the software composition of computer software which can have its identification in the network. It can communicate with sensor nodes in the network. Moreover it can move around the network repeatedly and serves its intended purpose of distributing keys. CH is responsible to sense data and also collects sensed data from other SNs. Thus the collected data is taken by CH and sends it to BS. The BS is assumed to have high computing and energy sources. This is the system model in which research is made in this paper to identify ways and means to have secure key distribution. Moreover, the keys are updated periodically in order to prevent known key and other attacks over WSN.

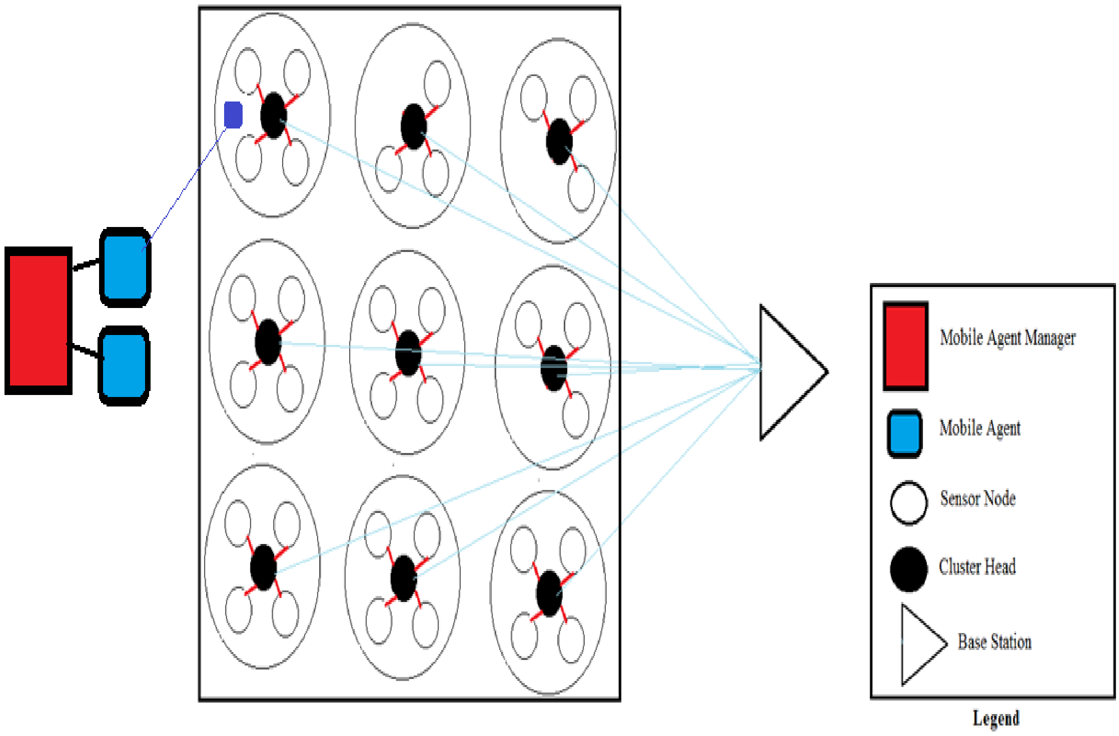

Figure 2. System Model

Key Agreement Protocol:

Table 1: Notations Used

Notation	**Description**
SN	Sensor Node
{n_A,n_B , n_C, ...)	Sensor nodes in WSN
N	Neighbour nodes
Pub$_A$	Public key of A
MA	Mobile Agent
KDA	Key Distribution Agent
(ID_A, ID_B, ID_C----)	IDs of sensor nodes
(RN_1,RN_2, RN_3---)	Random numbers
E	Encryption
M	Plain Text (Message)
D	Decryption
K$_{AB}$	Secret key

Algorithm: Agent Based Key Distribution (ABKD)

1. SN ϵ {n_A,n_B , n_C, ...)→N.
2. N nodes obtain Pub_A from MA (KDA);

   (ID_A, ID_B, ID_C----)with (RN_1,RN_2, RN_3---) →MA.
3. {n_A,n_B , n_c, ...)← Pub_A, Pub_B, Pub_C ---from MA.
4. n_A←E(Pub_A ,M) with { ID_A, ID_B, RN_1 }.
5. n_A = D(E(Pub_A ,M)).

   n_A gets RN of ID of N.

   E((n_A { K$_{AB}$, RN$_1$}), Pub$_B$) → n_B.
6. Complete verification.

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

$$X_0 = (X+1/2)L$$

$$Y_0 = (Y+1/2)L$$

IV. IMPLEMENTATION

The proposed scheme is implemented using NS2 which is a discrete event simulator widely used by computing world across the world. The simulator supports different types of wired and wireless protocols to in simulated environment. We have chosen this simulation tool as it can provide a means to test the proposed scheme in the laboratory environment prior to implementing in the real world sensor networks.

V. PERFORMANCE ANALYSIS

NS2 simulations are made with many experiments. The empirical study is made with 100 nodes to 1000 nodes increasing by 100 gradually. The results of the proposed key management system is compared with existing works in terms of computational overhead, communication overhead, memory overhead and resilience against node capture attacks.

Memory Overhead

Memory Overhead is the measure used to know how much main memory is consumed by WSN for execution of proposed key distribution scheme.

Memory usage depends on the number of neighbours. Memory usage of Key Management system does not depend on the number of nodes in the network. If there are N nodes in the Wireless Sensor Network and there are K neighbours in the network then the Memory overhead(M) is calculated as follows.

K*(public key size of mobile agent+ public key size of neighbour node+ private key size +Shared key size)

$M =(K *(\text{sizeof}(MA_{Pub}) + \text{sizeof}(N_{Pub}) + \text{sizeof}(S_{Pri}) + \text{sizeof} (S_{Sh}) + \text{sizeof}(S_{ID}))$

M= Memory overhead in Bytes

K=Number of Neighbours nodes

MA_{Pub} = Mobile agent Public Key

N_{Pub} = Sensor node Public Key

N_{Pri} = Sensor node Private Key

N_{Sh} = Sensor node Shared Key

S_{ID} = Node identifier

When number of nodes is increased, the memory usage is increases for the proposed scheme and Sahingoz [1] scheme. The memory consumed by the proposed scheme when number of nodes is 100 is 346 bytes while the scheme in [1] consumes 410 bytes for the same. In the same fashion when number of nodes is 1000, the proposed scheme consumes 430 bytes while that of [1] consumes 538 bytes. This trend is apparent for different number of nodes presented. This clearly indicates the efficiency of the proposed scheme with respect to optimal memory usage.

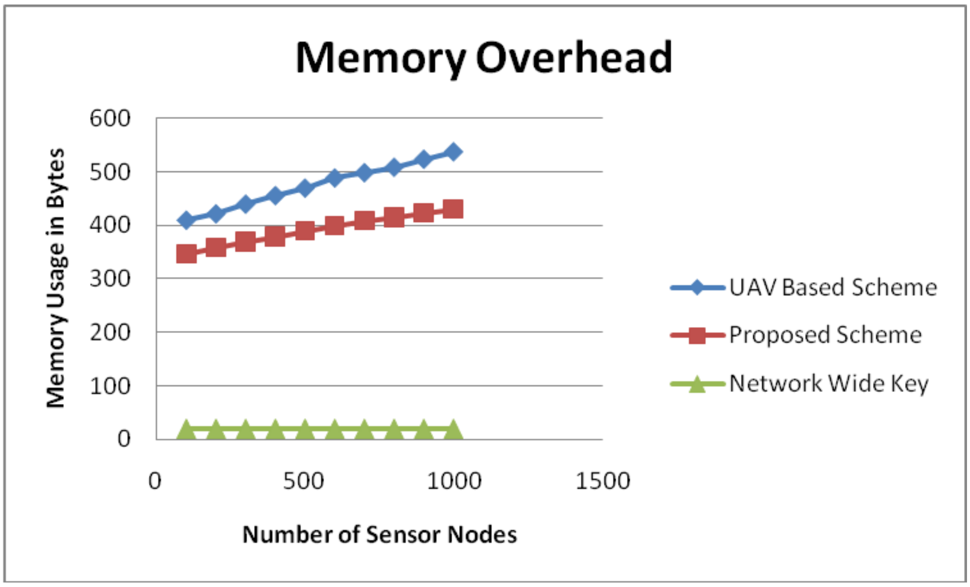

Figure 3. Memory Usage Dynamics of Different Key Distribution Schemes

Three key distribution schemes, as shown in Figure 5 are compared with respect to memory usage. It is understood that the Network Wide Key consumes very less memory as it make use of only one key for entire network. Apart from that two other trends are visible. The first trend is that the memory usage is directly proportional to number of nodes used in the simulation. The second trend is that the proposed scheme is consistently using less memory when compared with the scheme in [1] with all number of nodes.

Communication Overhead

It is a measure used to know how WSN causes overhead in communication. It is computed as follows.

In the proposed scheme, there is a communication overhead in the network initialization phase. Firstly, a sensor node should provide the public keys of the neighbours from the Mobile Agent. After that, this node should set up a shared key with its neighbours. It uses about 1090 bits additional communication overhead for setting up a shared key with a single neighbour.

If it assumed that there are 500 nodes of the system and 14 neighbours of each node, then it results 18,060 bits additional messaging for setting up shared keys for a node. If there are N nodes in the Wireless Sensor Network and there are P neighbours in the network

C= (1090 Bits*P)

C =Communication Overhead

P = Number of neighbours

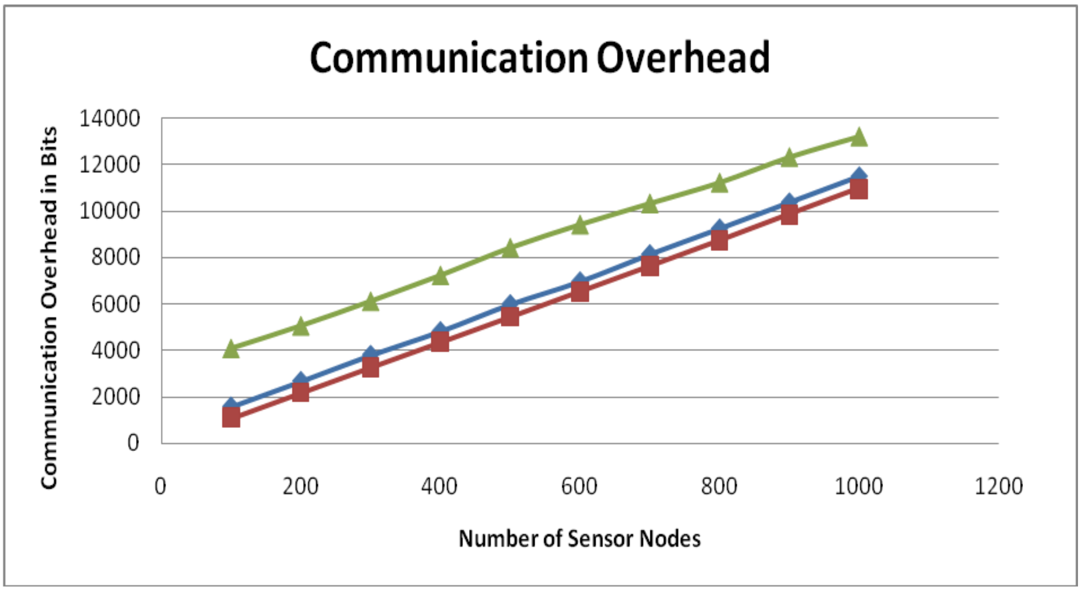

Figure 4. Number of Nodes vs. Communication Overhead for Different Schemes

The communication overhead, as shown in Figure 6 is more with public key scheme as it has more communication messages involved. In the same fashion, the scheme in [1] causes less overhead when compared with that of proposed scheme. When number of nodes is increased the communication overhead is also increased. The communication overhead is measured in number of bits. When number nodes is 100, the communication overhead caused by the three schemes is less while same is gradually increased when the number of nodes is increased by 100 till it reaches 1000.

Rate of Compromised Keys

It is the measure used to know the number of revealed rate of secret keys when a node is physically captured.

In the proposed scheme, each pair of two communicating nodes has a unique shared key. Therefore, if a sensor node is compromised, this does not affect other nodes in the system, except neighbors.

$$R = n / q$$

n= The number of neighbours of a node

q= The number of nodes in the system

R = Rate of Compromised keys

The network wide key scheme has the rate 0.08 and 0.05 when the number of nodes is 100 and 200 respectively. With all other experiments with different number of nodes it shows 0. In the same fashion, the proposed method shows 0.09, 0.07, and 0.03 when number of nodes is 100, 200 and 300. For all other experiments with different number of nodes, the proposed scheme shows 0. On the other hand, the scheme in [1] shows 1 as the rate of compromised keys in network for all experiments right from 100 nodes to 1000 nodes. Network wide key scheme shows superior performance when compared with the other schemes. The proposed scheme performs better than the scheme in [1].

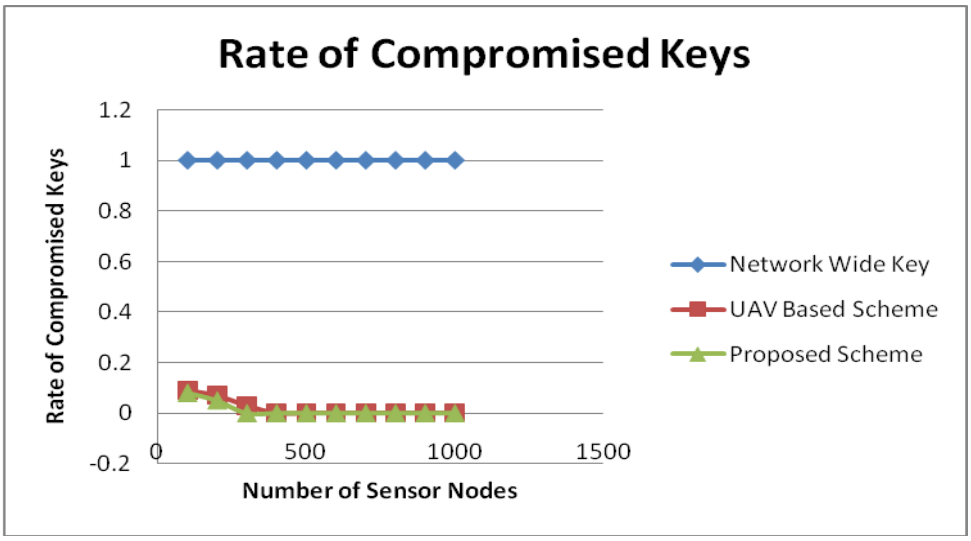

Figure 5. Rate of Compromised Keys in WSN

Computation Overhead

It is the measure used to find out overhead pertaining to computations involved in key distribution scheme. Excess or indirect or possible unnecessary computations cause overhead to WSN.

If there are N neighbours then in the proposed algorithm Computation Overhead(C) is calculated as follows.

C= N*6Encryptions/Decryptions

The computation overhead results reveal that the number of nodes in the network has its influence on the key distribution scheme. When the number of nodes is increases, the computation overhead is relatively increased. This trend is clearly visible in all the schemes. The public key scheme is causing more computation overhead when compared to that of proposed scheme and the scheme in [1]. The number of nodes is increased by 100 and the results are captured from 100 to 1000 nodes. The proposed scheme is causing less overhead when compared with the other two schemes. The rationale behind this is the optimization in the key distribution scheme which makes use of mobile agent.

When 100 nodes are in the network, the proposed scheme causes computation overhead in secs 0.2, scheme in [1] causes 1.1 secs while the public key scheme causes 1.4 secs. In the same fashion when the number of nodes is 1000, the proposed scheme, scheme in [1] and public key scheme cause overhead such as 1.1, 2.0 and 2.3 secs respectively. This trend is visible with all experiments done with different number of nodes in WSN.

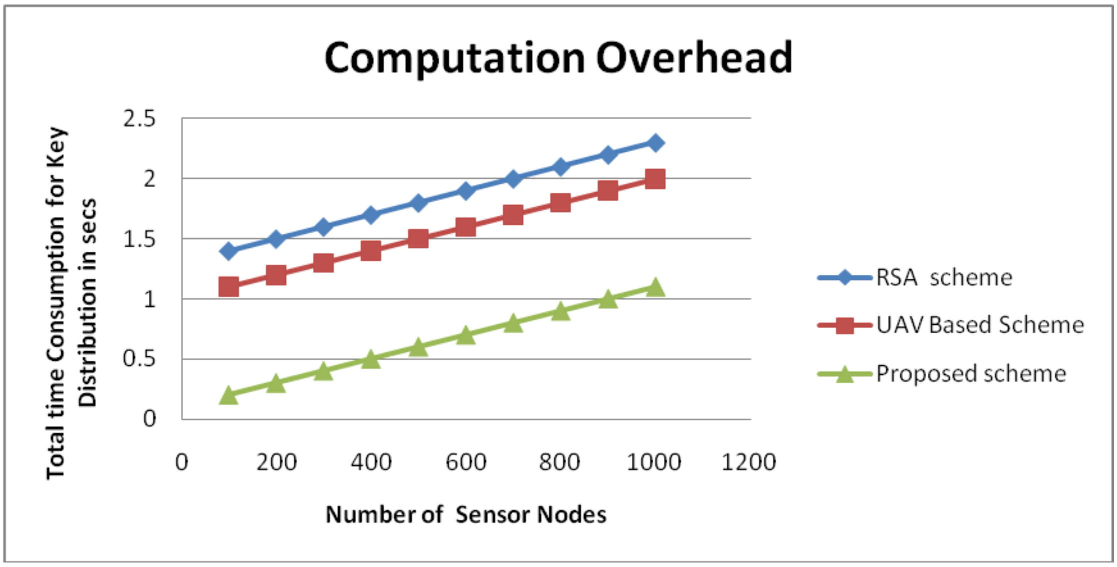

Figure 6. Time Consumption for Key Establishment

Energy Consumption

The Energy Consumption involved in the key agreement process, data transmission and reception.

In the proposed scheme Energy Consumption is calculated as follows.

$$E = A_T.k .\log_2 (|S|) + n. k.A_R.\log_2. (|S|)$$

A_T = The average energy consumed by the transmission of one bit

A_R = The average energy consumed by the reception of one bit

E = Energy consumption

S = Size of node identifier in bits

N = Average number of neighbours

k = Size of Public key

When the number of nodes is increases, energy consumptioon is relatively increased. This trend is clearly visible in all the schemes. The public key scheme is causing more energy consumption when compared to that of proposed scheme and the scheme in [1]. The number of nodes is increased by 100 and the results are captured from 100 to 1000 nodes. The proposed scheme is causing less energy consumption when compared with the other two schemes. The rationale behind this is the optimization in the key distribution scheme which makes use of mobile agent.

When 100 nodes are in the network, the proposed scheme causes energy consumption 156 mJ, scheme in [1] causes 189 mJ while the public key scheme causes 326 mJ. In the same fashion when the number of nodes is 1000, the proposed scheme, scheme in [1] and public key scheme cause energy consumption such as 248, 360 and 438 mJ respectively. This trend is visible with all experiments done with different number of nodes in WSN.

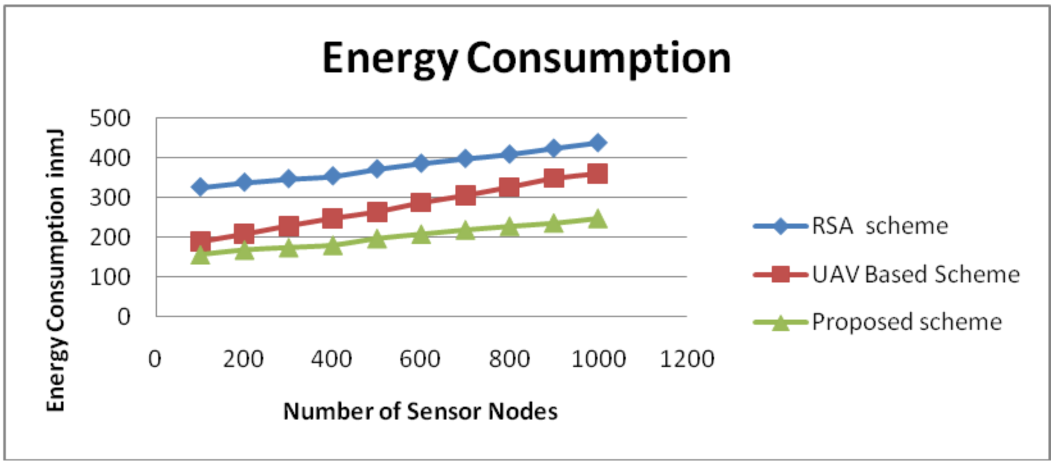

Figure 7. Energy Consumption

VI.CONCLUSION AND FUTURE WORK

This Research helped the author of the paper to explore dynamic key distribution scheme in dynamic WSN by exploiting mobile agent based approach as underlying mechanism. The following are the conclusions made.

Conclusion

Mobile Agent Based Secure and Dynamic Key Management Scheme (MASDKM) are proposed and implemented. It exploited 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, memory usage besides improving resiliency against node capture.

Future Scope

From the understanding of research insights the author of the thesis provides the following directions for future work.

- The agent based scheme proposed in this research needs to be evaluated against various kinds of attacks in WSN. The resiliency is thus further validated.
- As the IoT is emerging technological innovation with sensor networks as part of underlying digital world, it is very interesting to investigate how WSN can reach to the level of security expected.
- In the perspective of pervasive computing, the proposed key distribution scheme and its adequacy need to be investigated further as such computing phenomenon requires highly reliable and secure communications.

REFERENCES

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

[2] 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.

[3] 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.

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

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[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] 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.