Volume 6, Issue 11, November 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Efficient Agent Based Key Distribution Approach for Wireless Sensor Network

Ramu Kuchipudi
Department of CSE, VCE,
Hyderabad, India

Dr. Ahmed Abdul Moiz Qyser
Department of CSE, MJCET,
Hyderabad, India

Dr. V V S S S Balaram
Department of IT, SNIST,
Hyderabad, India

Abstract*— Security is given paramount importance in modern computing world. It must be true with Wireless Sensor Network (WSN) which is resource hungry. Moreover such networks run in hostile environment. As low-cost sensor networks became ubiquitous and used in different real world applications, it became indispensable to have secure key distribution mechanism in place. Of late, the usage of mobile agent assumed significance in communication networks for dissemination of data or collection of data efficiently. Mobile agent is encapsulates software and data moves autonomously from one node to another node in network. Thus it is found suitable for WSN to have cost-effective key distribution. The key idea of using mobile agent is that it travels in a pre-defined path to reach sensor nodes in its broadcasting range in order to distribute keys. In this paper we proposed a key distribution scheme that exploits the concept of mobile agent. The scheme makes use of symmetric cryptography between nodes. However the key exchange is made securely using asynchronous cryptography. The agent based key distribution has significance in this context as it can serve sensor nodes in distributing keys. The analysis revealed that the proposed scheme is efficient in terms of communication cost, computational cost, memory overhead and resilience against node capture attacks. Our NS2 simulations demonstrate the proof of concept. The results showed that the performance of the proposed scheme is better than many existing schemes.

***Keywords*— Wireless Sensor Network, authentication, dynamic key distribution, mobile agent**

I. INTRODUCTION

With innovations in electronics and computing technologies there is availability of low-cost sensing devices. This has caused the ubiquitous nature of WSN which is widely used in military and civil applications. Sensor networks are used in applications pertaining to health monitoring, study of animal and plant habitats, sensing natural calamities such as earth quake, tsunami, and cyclones, detection of explosives, and traffic control to mention few. As the nodes in WSN are resource hungry, they are vulnerable to attacks. To overcome security and privacy issues in WSN, an efficient key management system is needed. Such scheme should not be resource intensive. Stated differently, highly energy efficient key distribution scheme is needed to ensure longevity of WSN besides secure communications.

Generally key distribution involves key setup, initial distribution of keys, periodic key distribution and key revocation to get rid of the usage of compromised keys. The key distribution approaches are broadly classified into static and dynamic. In the static key distribution approaches keys are pre-loaded into sensor nodes before the network is deployed. Once the network is in place, all nodes have shared keys and they can communicate securely. There is no key update in the life of network. This approach has advantages such as no communication overhead after deployment and base station is excluded from key management. Its downside includes the probability of compromising keys which jeopardizes the interests of whole network and not suitable for dynamic WSN where nodes have mobility and there may be new nodes added and existing ones removed.

To overcome the issues of static key management, dynamic key management approaches came into existence. These schemes change master keys periodically so as to avoid known key attacks. The advantages of this scheme include improved network survivability, resilience, and support for network expansion. Disadvantages include communication overhead and demands highly efficient mechanisms for key distribution. 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. PROPOSED KEY DISTRIBUTION SCHEME

This section provides an overview of the proposed system model before presenting the proposed distribution scheme.

A. System Model

In this model, WSN is considered with sensor nodes forming into number of clusters. These sensors are built for particular purpose. They sense data from surroundings as per the purpose for which they are manufactured. Each cluster in network is denoted as C(SN1, SN1, SN3,…). Each cluster has a special node with high energy sources. Such node is

known as Cluster Head (CH). A SN can capture data from surroundings and send the data to CH. In turn the CH communicates with base station. This is shown in Figure 1. The base station (BS) is considered to have rich energy and computing resources. It is the important node in the network that can serve queries on the sensed data. With innovative technologies that came up in the recent past, the BS can be connected to Internet server through gateway. Thus the whole WSN can participate in the new networking world known as Internet of Things (IoT). IoT is an emerging technology which makes use of many technologies in inter-disciplinary fashion. Thus WSN is going to play vital role in the real world for remote surveillance, healthcare, military, house hold monitoring, monitoring of animal and plant habitats, and even machine critical applications such as predication of cyclones, tsunami, earthquake and so on.

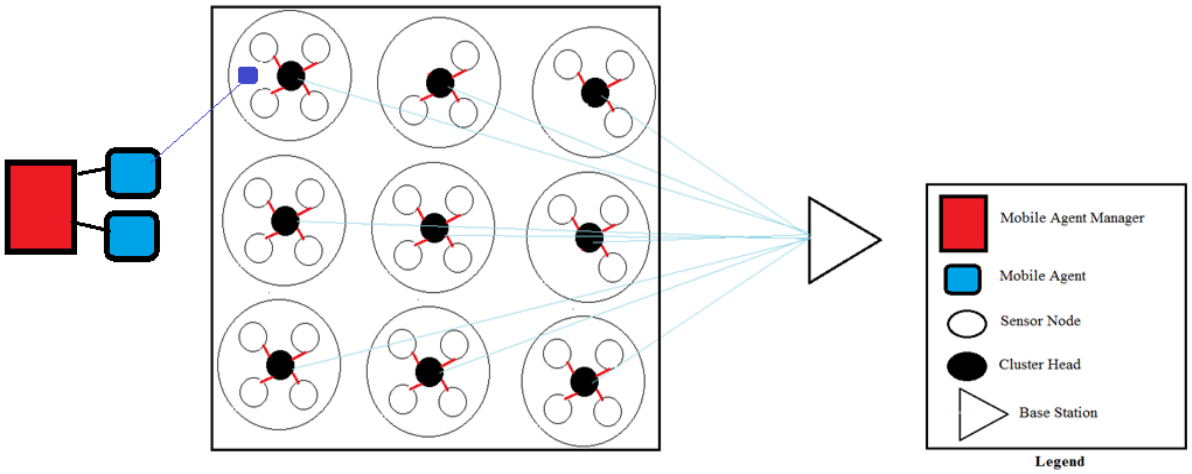

Fig.1. System Model

As shown in Fig 1, 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. When WSN is extended and integrated zith IoT infrastructure, it appears as shown in Fig 2.

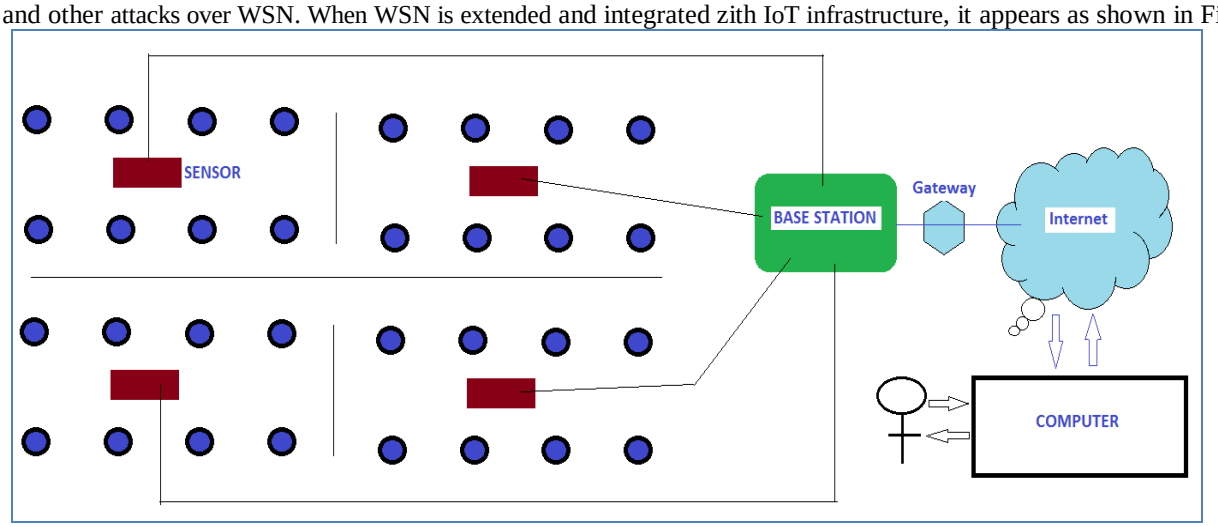

Fig. 2 Integration of WSN with IoT to Achieve Precision Agriculture

As illustrated in Figure 2, the blue circles are set of 8 trees that are under surveillance of a sensor node of WSN. All sensor nodes can have vital signs of trees and their needs to base station. Here the trees are things that can participate in the network as they can introduce themselves with Radio Frequency Identification (RFID). The RFID can uniquely identify things besides eliminating line of sight. The trees with RFID can help sensors to collect their data along with virtual identities of trees. This way Internet of Things is helping physical world of trees to be integrated with digital world of WSN and Internet. The BS is intern connected to Internet gateway and Internet. The people concerned with the network can be at any corner of the world and gain access to the sensed data. Particularly this scenario is pertaining to Precision Agriculture (PA) which is an inter-disciplinary approach which makes use of technologies to have real time

monitoring of agricultural fields to optimize inputs and outputs. The point being made here is that the proposed key distribution scheme can be used in this kind of scenario to protect communications in WSN. Since WSN can participate in Iota, protecting its communications is indispensable. Though this paper is not related IoT, the scenario should provide the context in which WSN can bestow value to the real word for real time monitoring of any target area.

As shown in Figure 1, the mobile agent is supposed to route through the network and provide public keys to sensor nodes as and when needed. MA is assumed to be trusted and resource rich. It can compute complex operations as well. MA moves according to a pre-defined path and provides public keys to sensors. Sensors are assumed to have private key that can be used to decrypt cipher text or encrypted messages. The keys are disseminated within its broadcasting range. The symmetric cryptographic approach is followed for ensuring secure communications. NS2 (Network Simulator) is a discrete event simulator that supports simulation of wireless networks such as WSN. The notations used in the proposed model are presented in Table 1.

Table 1 Notations Used In The Proposed Scheme

NOTATION	DESCRIPTION
L	Network latency
S	Data to be transferred
R	Compression ration
B	Network bandwidth
C	Compression time
I_A	ID of ALICE
I_B	ID of BOB
P1,p2,q1,q2	Prime integers
N	Modulus of public and private key
ø(n)	Euler's totient function
E	Public key exponent
D	Private key exponent
Pub_B	Public key of BOB
pub_A	Public key of ALICE
E	Encryption
C	Cipher text
P	Plain text
D	Decryption
K_{AB}	Shared Key
Prv_B	Private Key of BOB

In the proposed model there is communication between sensor node and MA. Two sensor nodes also can communicate each other securely by establishing a shared key. The mobile agent based secure key distribution is explored in this paper. When sensor nodes have their private key and public key known, they are supposed to get the public key of other node to which they need to communicate secure. For each sensor node public key is provided by MA. Then the node named Alice gets the node Bob's public key from MA. Then the two nodes can have mutual shared key. The mechanism is presented in Fig 3.

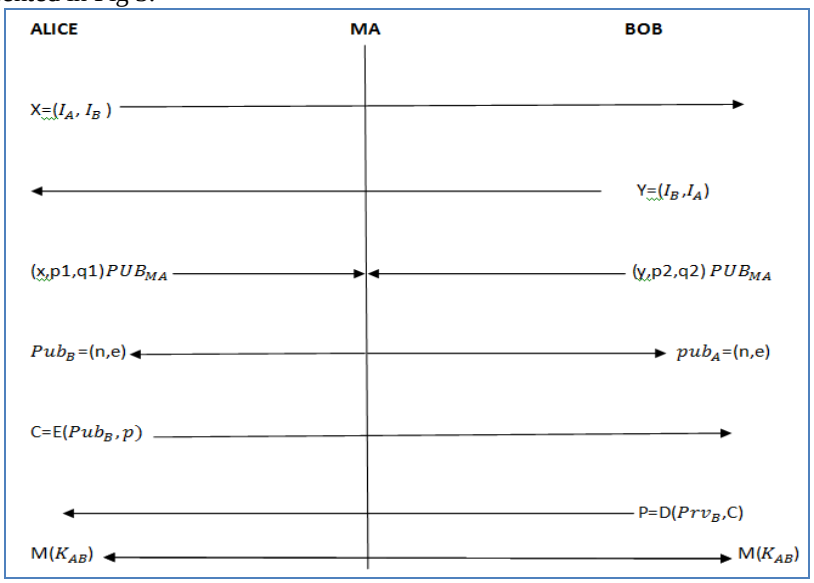

Fig.3 Mobile Agent Based Key Distribution Scheme

Prior to elaborating each step in the proposed key distribution scheme, here is the brief description of it. First of all Alice sends her ID to Bob. Then Bob sends his ID to Alice. Thus two nodes are able to exchange IDs to each other. Afterwards Alice or Bob can make a request to MA for other node's public key. On receiving such request MA computes public key of the node whose public key is requested. Then MA sends it to the node requested in secure fashion. Once Alice gets public key of Bob, she can send encrypted message to Bob. Alice uses public key of Bob, the recipient, to encrypt message. On receiving encrypted message from Alice, Bob uses his private key to decrypt the message. This is the beauty of public key or symmetric key encryption where key sharing is avoided. Since the public key and private key combination are with both sender and receiver there is no need to share a key in network on the fly which is vulnerable to attacks. The graphical view of the process in which two keys are used for encryption and description is shown in Figure 3.

B. Obtaining Public Key of Neighbour from MA

Alice sends her ID to Bob.

X=(I_A,I_B) (1)

After receiving Alice ID, Bob sends his ID to Alice.

Y=(I_B,I_A) (2)

Alice sends request to MA for public key of Bob. For this Alice needs to choose two prime integers denoted as p1 and q1.

The request made by Alice is represented as follows. (X,p1,q1)PUB_{MA} (3)

In the same fashion, Bob can also get public key of Alice from MA. For this, Bob sends request to MA for public key of Alice. For this Bob needs to choose two prime integers denoted as p2 and q2. The request made by Alice is represented as follows.

(Y,p2,q2)PUB_{MA} (4)

MA on receiving a public key request from Alice or Bob computes n and ø where n denotes a value which is the multiplication of p and q and ø denotes totient function.

n=pq (5)

The totient function is computed as follows.

ø(n)=(p-1)(q-1) (6)

where ø(n) is known as Euler's totient function.

Then MA computes public key exponent e that much be a coprime number to ø(n) i.e. 0<e< ø(n). It also should satisfy the condition Gcd(e, ø(n))=1 where Gcd is nothing but greatest common divisor. Thus correct public key exponent is obtained.

C. Encryption

Alice or Bob can send encrypted messages to each other. For instance, Alice wants to send a message m to Bob. Then the encryption process is denoted as follows.

C (m)= m^e mod n (7)

where e is known as public key exponent and n is the one computed in equation (5). C(m) represents cipher text or the encrypted message while m represents message. The whole encryption process is represented as follows.

C=E(Pub_B, p) (8)

D. Decryption

After receiving encrypted message, Bob uses his private key to decrypt the message. The decryption process is done as follows.

m(C)=c^dmod n (9)

where d is private key exponent of Bob which can be computed as follows.

d*e mod (ø(n))=1 (10)

The whole decryption process can be denoted as follows.

P=D(Prv_B,C) (11)

III. IMPLEMENTATION AND RESULTS

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.

Table 2 Simulation Environment Used

Sl. No.	Parameter Type	Parameter Value
1	Channel type	Channel/WirelessChannel
2	Radio-propagation model	Propagation/TwoRayGround
3	Antenna type	Antenna/OmniAntenna
4	Link layer type	LL
5	Interface queue type	DropTail
6	Network interface type	Phy/WirelessPhy
7	MAC type	Mac/802_11
8	Routing Protocol	AODV
9	Number of Mobile Nodes	20
10	Network Area	1000 x 1000
11	Interface Queue Size	50
12	RTSThreshold_	3000

The simulation environment is shown in Table 2. The proposed scheme is implemented and tested to demonstrate the proof of concept. Many performance metrics are used to evaluate the proposed work.

A. Communication Overhead

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

Communication overhead = $2L + \frac{S}{BR} + C$

where L denotes network latency, S denotes data to be transferred, R denotes compression ratio, B denotes network bandwidth and C denotes compression ratio.

B. 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.

C. Memory Overhead

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

D. Resilience against Node Capture

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

E. Results and Discussion

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.

Table 3 Memory Usage (Bytes) Of Different Schemes

NUMBER OF NODES	SAHINGOZ [18]	PROPOSED	NETWORK WIDE KEY
100	410	340	20
200	420	350	20
300	430	360	20
400	440	370	20
500	450	380	20
600	460	390	20
700	470	400	20
800	480	410	20
900	490	420	20
1000	500	430	20

The results presented in Table 3, show the performance of proposed scheme and other schemes to which it is compared. When number of nodes is increased, the memory usage is increases for the proposed scheme and Sahingoz [18] scheme. Interestingly, this trend is not true with Network Wide Key scheme where only one key is used for the entire network. It is consuming 20 bytes consistently when number of nodes is increased by 100 from initial 100 nodes to 1000 nodes. Therefore the Network Wide Key scheme outperforms all other schemes for the same reason. When the proposed scheme is compared with that of [18], it is understood that the proposed scheme outperforms the scheme in [18]. The memory consumed by the proposed scheme when number of nodes is 100 is 340 bytes while the scheme in [18] 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 [18] consumes 500 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.

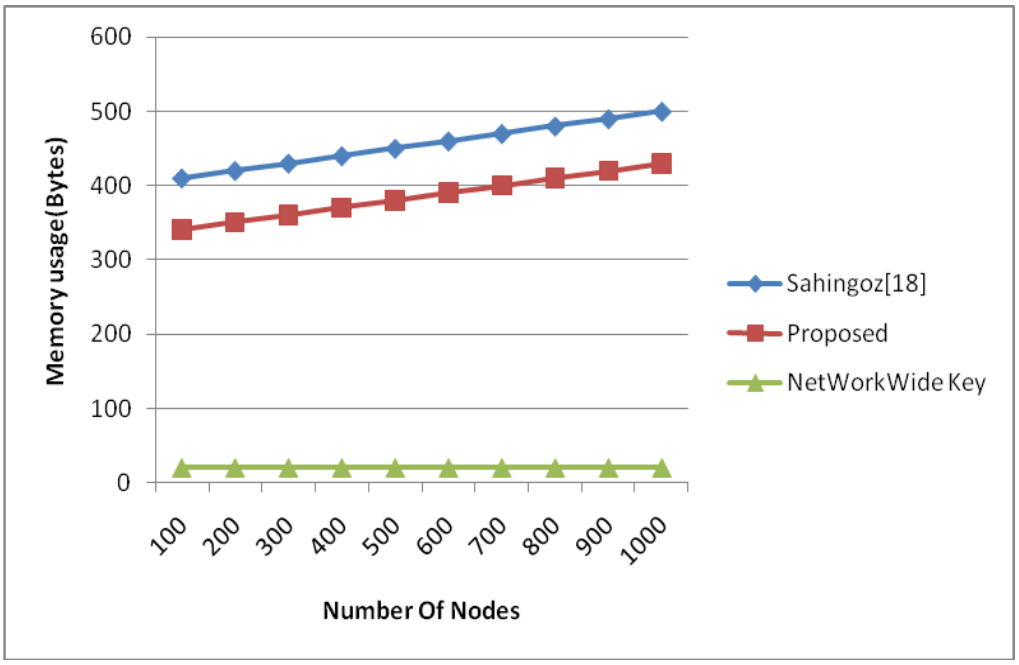

Fig. 4 Memory Usage Dynamics of Different Key Distribution Schemes

Three key distribution schemes, as shown in Figure 4, 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 [18] with all number of nodes.

Table 4 Performance (Communication Overhead) Comparison Of Different Schemes

	COMMUNICATION OVERHEAD IN BITS		
NUMBER OF NODES	**SAHINGOZ [18]**	**PROPOSED**	**PUBLIC KEY**
100	1200	600	2700
200	1400	700	3000
300	1600	800	3500
400	1800	900	3700
500	2000	1000	4500
600	2200	1100	4800
700	2400	1200	5000
800	2600	1300	5300
900	2800	1400	6000
1000	3000	1500	6200

As shown in Table 4, the performance of three schemes is compared in terms of communication overhead. The communication 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 communication overhead is relatively increased. This trend is clearly visible in all the schemes. The public key scheme is causing more communication overhead when compared to that of proposed scheme and the scheme in [18]. 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 communication overhead in bits 600, scheme in [18] causes 1200 while the public key scheme causes 2700. In the same fashion when the number of nodes is 1000, the proposed scheme, scheme in [18] and public key scheme cause overhead such as 1500, 3000 and 6200 respectively. This trend is visible with all experiments done with different number of nodes in WSN.

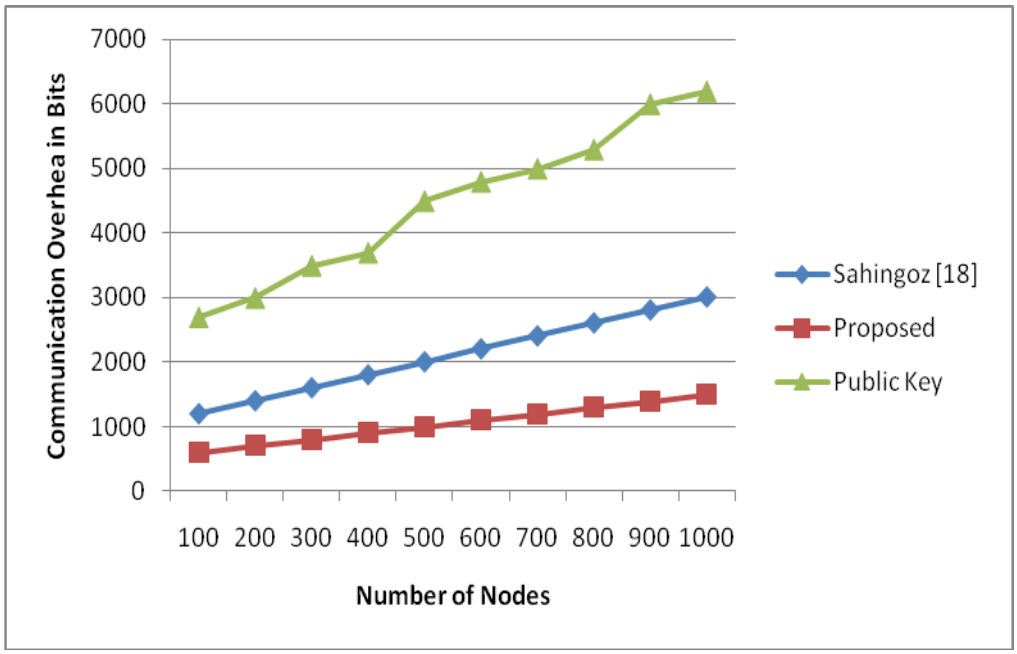

Fig.5 Number of Nodes vs. Communication Overhead for Different Schemes

The communication overhead, as shown in Figure 5, is more with public key scheme as it has more communication messages involved. In the same fashion, the scheme in [18] 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. The bottom line here is that number of nodes in the network has its influence on the communication overhead and the proposed scheme outperforms other schemes studied. These insights are useful in making decisions while using different security schemes.

Table 5 Shows Rate Of Compromised Keys In WSN

NUMBER OF NODES	SAHINGOZ [18]	PROPOSED	NETWORK WIDE KEY
100	1	0.09	0.08
200	1	0.07	0.05
300	1	0.03	0
400	1	0	0
500	1	0	0
600	1	0	0
700	1	0	0
800	1	0	0
900	1	0	0
1000	1	0	0

Rate of compromised keys, as shown in Table 5, reveals the fact that three schemes are compared with the values for rate of compromised keys in WSN. 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 [18] 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 [18].

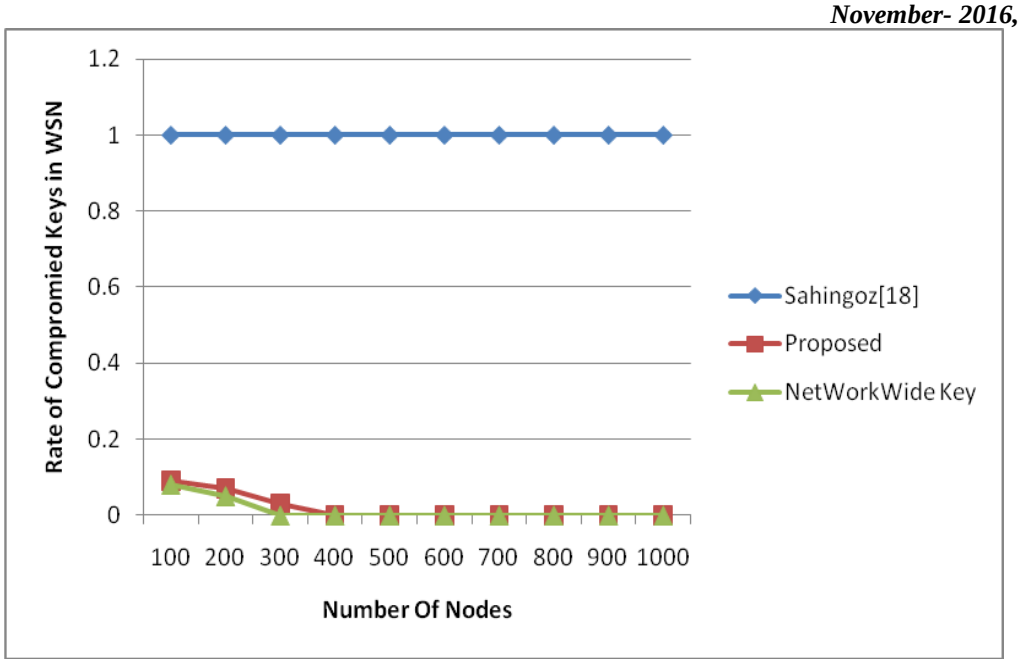

Fig.6 Rate of Compromised Keys in WSN

The rate of compromised nodes in WSN is presented in Figure 6. It is evident that the rate is high with the scheme in [18]. There is comparable difference between the network wide scheme and the proposed scheme. The proposed scheme shows better performance when compared with that of [18]. However, the performance of network wide key is better than the other two schemes. The empirical results are considered for nodes 100 to 1000 incremented by 100 gradually. Interestingly the number nodes has no influence over the scheme in [18] as it shows same rate for all range of nodes that is from 100 to 1000. This is not true with the other two schemes as they had varied performance when number of nodes is increased. When nodes are beyond 200, the network wide key showed zero rate of compromised keys while the proposed scheme does so when number of nodes is beyond 300.

IV. CONCLUSION AND FUTURE WORK

In this paper we have proposed a key management scheme for resource hungry WSN. The proposed scheme employs mobile agent for secure key distribution. Mobile agent is software component which moves across a pre-defined path in WSN to disseminate keys required by sensor nodes. As the concept of mobile agent is becoming an attractive solution for data gathering of dissemination, in this paper, we proposed a mobile agent which is meant for key effective distribution. Symmetric cryptography is preferred between nodes in the network. However the key exchange involved in the symmetric approach leverages the presence of asymmetric cryptography that is used by nodes in order to have secure key establishment.

The agent based key distribution has significance in this context as it can serve sensor nodes in distributing keys. The analysis revealed that the proposed scheme is efficient in terms of communication cost, computational cost, memory overhead and resilience against node capture attacks. We implemented the proposed scheme using NS2 simulations. The results revealed that the scheme has comparable performance improvement over other schemes such as [18], public key and network wide key in terms of communication overhead, memory overhead and the rate of compromised keys in WSN.

REFERENCES

[1] Haowen Chan. (2003). Random Key Predistribution Schemes for Sensor Networks. *IEEE*, p1-23.

[2] Wenliang Du. (2006). Key Predistribution Scheme for Sensor Networks Using Deployment Knowledge. *IEEE*. 3 (1), p1-23.

[3] WENLIANG DU. (2005). A Pairwise Key Predistribution Scheme for Wireless Sensor Networks. *ACM Transactions on Information and System Security*. 8 (2), p1-16.

[4] Sk.Md. Mizanur Rahman. (2010). Private key agreement and secure communication for heterogeneous sensor networks. *Elsevier*. 70, p.858-870.

[5] Kejie Lu. (2008). A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks. *IEEE*. 7 (2), p1-18.

[6] David Sánchez Sánchez. (2005). A Deterministic Pairwise Key Pre-distribution Scheme for Mobile Sensor Networks. *IEEE*, p1-10.

[7] I-Hsun Chuang. (2007). Two-layered Dynamic Key Management in Mobile and Long-lived Cluster-based Wireless Sensor Networks. *IEEE*, p1-16.

[8] Sarita Agrawal. (2012). A Novel Key Update Protocol in Mobile Sensor Networks. *Springer-Verlag London Limited*. 12 (1), p. 194–207.

[9] Sarmad Ullah Khan. (2011). An Energy and Memory-Efficient Key Management Scheme for Mobile Heterogeneous Sensor Networks.*Department of Computer Science*, p1-23.

[10] SEYIT A. C¸AMTEPE. (2002). Key Distribution Mechanisms for Wireless Sensor Networks: a Survey. *Department of Computer Science*, p1-16.

[11] Nils Gura. (2004). Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs. *Department of Computer Science*, p.119–132.

[12] Sattam S.. (2003). Certificateless Public Key Cryptography.*Department of Computer Science*, p. 452–473.

[13] Seung-Hyun Seo. (2005). Elliptic Curve Cryptography based Certificateless Hybrid Signcryption Scheme without Pairing.*Department of Computer Science*, p1-16.

[14] Seung-Hyun Seo. (2014). POSTER: A Pairing-free Certificateless Hybrid Sign- Cryption Scheme for Advanced Metering Infrastructures.*Department of Computer Science*, p1-18.

[15] Qiang Huang. (2003). Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks. *Department of Computer Science*, p1-9.

[16] Xi-Jun Lin. (2013). Cryptanalysis and improvement of a dynamic and secure key management model for hierarchical heterogeneous sensor networks. *P.R chinna*, p.793-801.

[17] Piotr Szczechowiak. (2008). NanoECC: Testing the Limits of Elliptic Curve Cryptography in Sensor Networks. *Department of Computer Science*, p. 305–320.

[18] Kakali Chatterjee. (2012). An Improved ID-Based Key Management Scheme in Wireless Sensor Network. *Department of Computer Science*, p.609–617.

[19] Wen Tao Zhu. (2012). Detecting node replication attacks in mobile sensor networks: theory and approaches. *John Wiley & Sons, Ltd*, p.54-76.

[20] Ian F. Akyildiz. (2002). A Survey on Sensor Networks. *IEEE*, p.793-801.

[21] Peng Jiang. (2009). A New Method for Node Fault Detection in Wireless Sensor Networks. *ISSN*, p.84–106.

[22] Lilia Paradis. (2007). A Survey of Fault Management inWireless Sensor Networks. *Department of Computer Science*. 15 (2), p.338--353 .

[23] An Liu. (2008). TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks. *IEEE*, p1-23.

[24] Jianmin Zhang, Qingmin Cui. (2008). An Efficient Key Management Scheme for Wireless Sensor Networks in Hostile Environments.*Department of Computer Science*, p1-23.

[25] Xiaobing He. (2012). Dynamic key management in wireless sensor networks: A survey. *Department of Computer Science*, p.54-76.

[26] Giacomo de Meulenaer. (2008). On the Energy Cost of Communication and Cryptography in Wireless Sensor Networks. *IEEE*, p.533–544.

[27] QAMAR TOHEED HASSAN RAZI. (2010). Asymmetric-Key Cryptography for Contiki. *Department of Computer Science*, p1-23.

