International Journal of Engineering & Technology, 7 (4.6) (2018) 45-48

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Energy efficient Key Distribution for Wireless Sensor Networks

Ramu Kuchipudi[1]*, Dr. Ahmed Abdul Moiz Qyser[2], Dr. V V S S S Balaram[3] A Manusha Reddy[4]

[1] Department of CSE, Vardhaman College of Engineering, Hyderabad,India
[2] Department of CSE, MJCET,Hyderabad, India
[3] Department of IT, SNIST, Hyderabad, India
[4]Department of Computer Science and Engineering MLR Institute of Technology, Hyderabad
** Corresponding Author E-mail: kramupro@gmail.com*

Abstract

Key distribution in Wireless sensor networks is crucial whenever they deployed in critical applications. Cryptography is used to protect sensitive information from disclosure. Key management is important component in cryptography. Cryptography is not useful if keys are disclosed to attackers. Designing an efficient key management for sensor network is a difficult task because of scarcity of computing and memory resources. An efficient key distribution approach is proposed by using mobile agent paradigm rather than client server model. The proposed approach will use good features of both symmetric and asymmetric cryptography. Mobile Agents are used to generate public and private key pairs, update keys and revocation of keys. The proposed scheme in the first level will use mobile agents for public key dissemination and in second level sensor nodes can involve in constructing symmetric keys for secure communication through mutual authentication and encryption with those keys. The proposed method is implemented using NS2 Simulator and results are compared with existing similar methods in terms of evaluation parameters like throughput and resiliency. The proposed method is improved when it is compared with similar existing methods**.**

Keywords: *Key Distribution; Mobile Agents; Wireless Sensor network*

1. Introduction

Designing an efficient key distribution mechanism in Wireless Sensor Network (WSN) is required to provide secure communications. Some of the applications of WSNs are healthcare monitoring, property surveillance, forest fire detection, study of wild life habitat, and enemy intrusion detection etc.

Cryptography has been used to provide secure communications in networks. But it is not feasible to use existing cryptographic key distribution mechanisms due to constraint resources. The key distribution is seen as efficient if it less communication overhead, computation overhead and memory overhead.

Different approaches are proposed in the existing literature like Key pre-distribution schemes, Self enforcing schemes and trusted server schemes to overcome resource scarcity problem. Key are predistributed in sensor node's memory before their deployment and secret keys are established between sensor nodes. Secret keys are generated and distributed among sensor nodes using server in trusted server schemes.

An efficient and secure key management for both static and dynamic WSN is a problem to be addressed. The existing approaches are used different mechanisms for key distribution in WSN. In that scheme hybrid key management approach is used wherein mobile certification authority is used to distribute public keys and by using public keys secret keys are distributed. In Sahingoz[1] approach mobile certification authority has to interact with each and every sensor node separately which increases communication overhead. Alternative method is required to reduce communication overhead further.

Mobile agents for key distribution in WSN are the research area little explored.

In proposed method mobile agent is used to distribute and update secret keys.

2. Literature Review

There are two types of key distribution mechanisms in the existing literature. Each sensor node can obtain shared keys from its neighbors. A sensor node is capable of setting up a shared key using intermediate nodes. Security of network is lost when the static keys are compromised.

Session keys are established using the preloaded keys in the sensor nodes in dynamic key management. Here keys are changed dynamically and for adversaries it is not easy to break security.

Gu *et al*. [2] 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*. [7] improved the authentication mechanism and prevented replication attacks. Khan *et al*. [8] proposed a KP scheme for WSN which is memory efficient and matrix-based. The scheme provides high scalability and network connectivity.

The scheme made use of enhanced unital-based approach with less storage overhead. Ruj *et al*. [10] 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 pair-wise and triple key establishment is used to have secure data aggregation in WSN. 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.
The work in 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 a scheme that makes use of mobile agent for public key distribution. The scheme reduces communication overhead, memory overhead and computational overhead. Besides, it is resilient against node capture attacks.

3. Proposed method

3.1Assumptions made

BS is trusted node which stores details of sensor nodes. Mobile agent is also assumed trusted component. The nodes of sensor network can be both static and dynamic. Signal range of all nodes does not exceed the threshold value. Other attacks like black hole, hello flood and wormhole attack possible.The research methodology followed is described here. The secondary research with literature review revealed useful insights. They include the issues with static key management schemes and advantages of dynamic key management schemes in terms of providing secure communications in WSN. Mobile agent based key distribution is explored in this research as part of dynamic key management scheme for WSN. The proposed methodology is presented in Figure1.

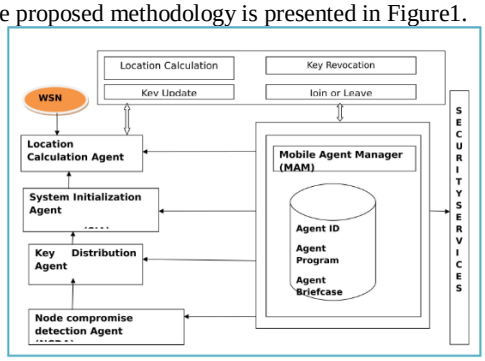

Fig.1: Overview of the Proposed Methodology

In the proposed system the initial stage is to run System Initialization Agent (SIA) to generate and stores public and private key pairs in all sensor nodes. Then LCA is executed to store location information of sensor nodes. Later Key Distribution Agent (KDA) and Node Compromise detection Agent (NCDA) algorithms are run to establish, update and revoke keys respectively.
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 System Initialization Agent.
(SIA), Location Calculation Agent(LCA),Key Distribution Agent (KDA) and Node Compromise detection Agent (NCDA).
System Initialization Agent (SIA) SIA generates and stores public and private key pairs in all sensor nodes using RSA Key generation algorithm**.**
LCA agent updates location information of sensor nodes whenever it visits them. The location information is used by the KDA which is responsible to provide public keys of neighbour nodes to sensor nodes.
Key Distribution Agent (KDA) checks public Key information on sensor nodes and compare it with its briefcase if they are not same pubic key information will be updated on sensor nodes. Then shared keys are established between a sensor node and neighbour nodes using those public keys. Sensor nodes will PRF to generate shared keys.
Key Distribution Agent (KDA) is used to update secret keys and public and private keys periodically and it is also invoked by agent manager whenever nodes join or leave the sensor network. Node compromise detection Agent (NCDA) is used to detect and isolate them from network. The NCDA calls KDA to update keys.

3.2 Pre deployment Phase

Before the network deployment BS assigns a unique identifier to all sensor nodes.
BS generates Public and Private Key pairs of Mobile Agents.
After generating Public and Private Key pairs the BS preloads them into Mobile Agents. Cluster Heads and Mobile Agents also contain the public key of the BS.BS launch mobile agents into network and each CH is given mobile agent.

3.3 Cluster formation Algorithm

Cluster formation is an important phenomenon in WSN. Sensor nodes in the network are grouped together in a geographical area to form a cluster which is headed by CH. CH nodes communicate with base station.
An algorithm is proposed to achieve this. The algorithm is responsible to ensure that right SN is chosen as CH.

Algorithm: Cluster Head Selection Algorithm
Initialize ***minDistance*** to hold minimum distance between cluster-head nodes
Initialize ***numClusters*** to hold number of cluster heads
Initialize ***numNodes***
Initialize ***avgEnergy***
Initialize ***CH***
Computer **avgEnergy** of remaining nodes
Find ***eligibleNodes*** as nodes with energy more than ***avgEnergy***
For each node ***n*** in **eligibleNodes**
IF |***CH***| < numClusters AND ***n*** satisfies ***minDistance*** THEN
Add ***n*** to ***CH***
Remove ***n*** from ***eligibleNodes***
ELSE
Remove ***n*** from ***eligibleNodes***
END IF
End For
The cluster head selection algorithm makes use of two important variables. They are average energy and minimum distance to make decision on cluster head selection. The algorithm initializes variables that hold minimum distance, number of clusters, number of nodes, and average energy. It computes average energy of remaining nodes. Later on there is an iterative process that employs criteria such as minimum distance and number of clusters for choosing final CH selection. The threshold for determining cluster head selection is computed as follows.

3.4 Location Calculation Agent (LCA) Algorithm

This is the mechanism used by LCA which is employed by MAM. Any pair nodes are decided as neighbor nodes based on the following steps.

- Let (x_i, y_j) and (x_k, y_m) be the original positions of two sensor nodes A and B.
- Calculate Distance between two sensor nodes $d = \sqrt{(x_k - x_i)^2 + (y_m - y_j)^2}$
- Calculate $\frac{R-d}{V}$ Where V=Average speed of the node
- If $\left(\left(\frac{R-d}{V}\right) <= Transmission\_Range\right)$ then A and B are treated as neighbor sensor nodes.

3.5 Key Distribution Agent Algorithm

Select two large primes p and q such that $p \neq q$.

$$n \leftarrow p \times q$$

$$\phi(n) \leftarrow (p-1) \times (q-1)$$

Select e such that $1 < e < \phi(n)$ and e is coprime to $\phi(n)$

$d \leftarrow e^{-1} \bmod \phi(n)$ // d is inverse of e modulo $\phi(n)$

$public\_key \leftarrow (e,n)$ // To be announced publicly

$private\_key \leftarrow d$ // To be kept secret

return $SN_{PU} \leftarrow public\_key$ and $SN_{PR} \leftarrow private\_key$

$RSA\_Encryption(M,e,n)$ // M is the plaintext in Z_n

{

$C \leftarrow M^e \bmod n$

return C

}

$RSA\_Decryption(C,d,n)$ // C is the Ciphertext in Z_n

{

$M \leftarrow C^d \bmod n$

return M

}

I. KDA updates public keys of Neighbor nodes

II. Secret Key K_{AB} generated by SN using PRF-MD5.

$$SN \leftarrow N : E\left(N_{PU}, (K_{AB} \square RN)\right)$$

$$D_{N_{PR}}\left(E\left(N_{PU}, (K_{AB} \square RN)\right)\right)$$

III. Data M is transmitted between SN and N encrypted using secret key K_{AB}

$$SN \rightarrow N : E_{K_{AB}}(M)$$

$$N \rightarrow SN : D_{K_{AB}}(M)$$

The key update is done based on the time elapsed based on a threshold. 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.

For every 24 hours KDA is initiated by Agent manager to update key information table of sensor nodes.

3.6 Performance & Security Analysis

The performance of proposed scheme is compared with existing schemes UAV Based scheme and HKM Scheme. When number of nodes is increased, the memory usage is increases as shown in fig. 5 for the proposed scheme and UAV Based scheme [1] scheme and HKM Scheme [19]. It is less in proposed scheme. The results are presented in terms of packet delivery ratio, packet dropping, throughput, delay and energy consumption based on number of nodes used in experiments. Mobile Agent Scheme outperforms HKM and UAV Based Schemes with respect to the percentage of data packets delivered.

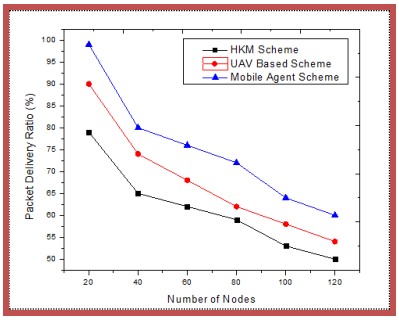

Fig.2: Number of Nodes Vs Packet Delivery Ratio

As shown in Figure 2, No. of nodes is represented on x-axis varies from 20 to 120 nodes. The packet delivery ratio is measured in percentage is taken on y-axis. As the no. of nodes increases, Mobile Agent, HKM and UAV Based schemes show decrease in packet delivery performance. However, the proposed Mobile Agent scheme outperforms the other schemes.

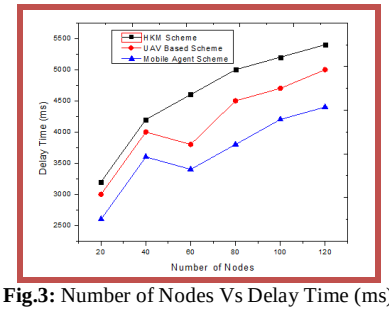

Fig.3: Number of Nodes Vs Delay Time (ms)

As shown in Figure 3, no. of nodes is taken on x-axis from 20 to 120 nodes and the delay time in milliseconds is taken in y-axis. The results show that Mobile Agent Scheme has better performance improvement over HKM and UAV Based schemes.

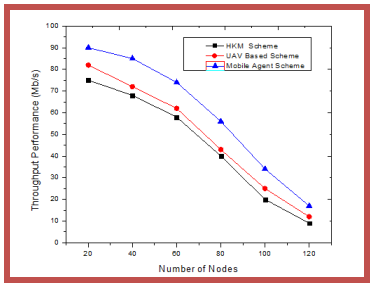

Fig.4: Number of Nodes Vs Throughput Performance (Mb/s)

As shown in Figure 4, as the number of nodes increased, the throughput performance is decreased in the network. However Mobile Agent scheme shows better performance than other schemes.

As number of nodes is increased the packet dropping is also increased however, HKM and UAV shows better performance than HKM and UAV schemes .The figure 5 shows, X- axis represents the number of nodes and Y- axis represents packet dropping ratio. From the graph it is evident that Mobile Agent scheme shows better performance than that of other existing schemes HKM and UAV Based schemes.

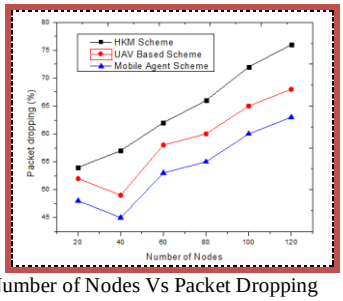

Fig.5: Number of Nodes Vs Packet Dropping

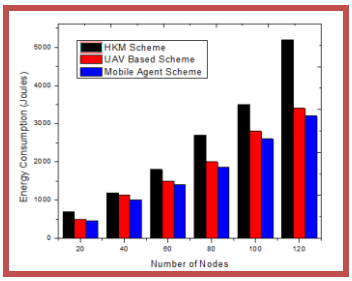

Fig.6: Number of Nodes Vs Energy Consumption

The Figure 6 presents the consumption of energy when number of nodes is increased. As the number of nodes increases, the consumption of energy increases. However proposed Mobile Agent Scheme shows energy efficiency when compared with other schemes.

The Proposed Key management is resist against attacks such as eavesdropping, Traffic Analysis, Spoofed or Replay and Node-compromise Attack. It is resist against eavesdropping attack due to encryption of secret keys.

Replay attack is handled by updating keys and nonce in key distribution messages. Node Compromise attack is tackled by key revocation. Due to periodic updating of secret keys and public keys traffic analysis is difficult.

Table 1 : Comparision of Security attacks

Attack	Proposed Scheme	UAV Based Scheme	HKM Scheme
Eavesdropping	Yes	Yes	Yes
Traffic Analysis	Yes	Yes	Yes
Node compromise Attack	Yes	No	No
Replay Attack	Yes	Yes	Yes

4. Conclusion

Mobile Agent Based Key distribution scheme is proposed. Mobile agents are used to generate, update and revoke keys. The dynamic key distribution is realized by using both symmetric and asymmetric cryptography. In the first level we introduced agent based key dissemination of public 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 when compared to the schemes in [1][19].

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. Author, *Title of the Book*, Publisher, (200X), pp:XXX-YYY.

[3] 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.

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

[5] Lai B, Kim S, Verbauwhede I. Scalable session key construction protocol for wireless sensor networks. In: Proceedings of the IEEE workshop on Large Scale RealTime and Embedded Systems LARTES, December 2002.

[6] Perrig A, Szewczyk R, Wen V, Cullar D, Tygar JD. SPINS: security protocols for sensor networks. In: Proceedings of the 7th annual ACM/IEEE international conference on mobile computing and networking, July 2001. p. 189–99.

[7] Chan H, Perrig A. PIKE: peer intermediaries for key establishment in sensor networks. In: Proceedings of the 24th annual joint conference of the IEEE computer and communications societies (INFOCOM '05), Miami, FL, USA, March 2005. p. 524–35.

[8] Chan H, Perrig A. Random key predistribution schemes for sensor networks. In: Proceedings of the 2003 IEEE symposium on security and privacy, May 2003. p. 197–213..

[9] Du W, Han YS, Chen S, Varshney PK. A key management scheme for wireless sensor networks using deployment knowledge. In: Proceedings of IEEE INFOCOM04. Hong Kong: IEEE Press; 2004. p. 586–97.

[10] Liu D, Ning P. Establishing HKM keys in distributed sensor networks. In: Proceedings of 10th ACM conference on computer and communications security (CCS03). Washington, DC: ACM Press; 2003. p. 41–7.

[11] Blom R. Theory and application of cryptographic techniques. In: Proceedings of the Eurocrypt 84 workshop on advances in cryptology. Berlin: Springer; 1985.p.335–8.

[12] Wallner D, Harder E, Agee R. Key management for multicast: issues and architectures, June 1999, RFC 2627.

[13] F. Anjum, Location dependent key management using random key predistribution in sensor networks, in: Proceedings of WiSe'06.

[14] S. Zhu, S. Setia, S. Jajodia, LEAP: efficient security mechanisms for large-scale distributed sensor networks, in: Proceedings of The 10th ACM Conference on Computer and Communications Security (CCS '03), Washington D.C., October, 2003.

[15] Camtepe SA, Yener B. Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Transactions on Networking (TON) 2007;15(2):346–58.

[16] Eltoweissy M, Heydari H, Morales L, Sudborough H. Combinatorial optimization of Group key management. Journal of Network and System Management 2004;12(1).

[17] Boneh D, Franklin M. Identity-based encryption from the weil pairing. In: Advance in cryptology-crypto, Lecture notes in computer science, vol. 2139, 2001. p. 213–29.

[18] Seo, Seung-Hyun, Won, Jongho, Sultana, Salmin, and Bertino, Elisa, Effective Key Management in Dynamic Wireless Sensor Networks. IEEE Transactions on Information Forensics And Security, 10 (2) (February 2015), 371 - 383.

[19] Pengcheng Zhao, Yong Xu, Min Nan, A Hybrid Key Management Scheme Based on Clustered Wireless Sensor Networks, Scientific Research(Aug 2012), 197-201Author,"Title of the Paper", *Journal name*, Vol.X, No.X, (200X), pp.XX-XX, available online: http://xxx, last visit:28.02.2013.