Dynamic Key Management in Wireless Sensor Networks

S.Silviya
M.Tech(IT), Dr.Sivanthi Aditanar College of Engineering, Tamilnadu, India.

N.Subbulakshmi
Assistant Professor, Department of IT, Dr.Sivanthi Aditanar College of Engineering, Tamilnadu, India.

Abstract – Wireless sensor networks have been deployed for a wide variety of applications. In this paper, we propose a certificateless-effective key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The CL-EKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy. The protocol also supports efficient key revocation for compromised nodes and minimizes the impact of a node compromise on the security of other communication links. A security analysis of our scheme shows that our protocol is effective in defending against various attacks.

Index Terms – Wireless sensor networks, certificateless public key cryptography, key management scheme.

1. INTRODUCTION

Dynamic wireless sensor networks, which enable mobility of sensor nodes, facilitate wider network coverage and more accurate service than static WSNs . However, sensor devices are vulnerable to malicious attacks such as impersonation, interception, capture or physical destruction, due to their unattended operative environments and lapses of connectivity in wireless communication [20]. Thus, security is one of the most important issues in many critical dynamic WSN applications. Dynamic WSNs thus need to address key security requirements, such as node authentication, data confidentiality and integrity, whenever and wherever the nodes move.

To address security, encryption key management protocols for dynamic WSNs have been proposed in the past based on symmetric key encryption. Such type of encryp- tion is well-suited for sensor nodes because of their limited energy and processing capability. However, it suffers from high communication overhead and requires large memory space to store shared pairwise keys. It is also not scalable and not resilient against compromises, and unable to support node mobility. Therefore symmetric key encryption is not suitable for dynamic WSNs.

In this paper, present a certificateless effective key management (CL-EKM) scheme for dynamic WSNs. In certificateless public key cryptography (CL-PKC) [12], the user's full private key is a combination of a partial private key generated by a key generation center (KGC) and the user's own secret value. The special organization of the full private/public key pair removes the need for certificates and also resolves the key escrow problem by removing the responsibility for the user's full private key. We also take the benefit of ECC keys defined on an additive group with a 160-bit length as secure as the RSA keys with 1024-bitlength

CL-EKM is scalable in case of additions of new nodes after network deployment. CL-EKM is secure against node compromise, cloning and impersonation, and ensures forward and backward secrecy. The security analysis of our scheme shows its effectiveness. Below we summarize the contributions of this paper:

- The security weaknesses of existing ECC based key management schemes for dynamic WSNs.
- Propose the first certificateless effective key management scheme (CL-EKM) for dynamic WSNs. CL-EKM supports four types of keys, each of which is used for a different purpose, including secure pair-wise node communication and group-oriented key supporting node movements across different clusters and key revocation process for compromised nodes.supporting node movements across different clusters and key revocation process for compromised nodes communication within clusters.

2. RELATED WORK

Symmetric key schemes are not viable for mobile sensor nodes and thus past approaches have focused only on static WSNs. A few approaches have been proposed based on PKC to support dynamic WSNs. Thus, in this section, we review previous PKC-based key management schemes for dynamic WSNs and analyze their security weaknesses or disadvantages.Chuang et al. [7] and Agrawal et al. [8] proposed a two-layered key management scheme and a dynamic key update protocol in dynamic WSNs based on the Diffie-Hellman (DH), respectively. However, both schemes [7], [8] are not suited for sensors with limited resources and are unable to perform expensive computations with large key sizes (e.g. at least 1024 bit). Since ECC is computationally more efficient and has a short key length (e.g. 160 bit), several approaches with certificate [5], [10],[15], [25] have been proposed based on ECC.

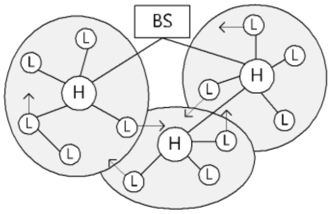


Fig.1.Heterogeneous dynamic wireless sensor network.

However, since each node must exchange the certificate to establish the pairwise key and verify each other's certificate before use, the communication and computation overhead increase dramatically. Also, the BS suffers from the overhead of certificate management. Moreover, existing schemes [5], [10],[15], [25] are not secure. Alagheband et al. It uses the symmetric key approach for sharing the pairwise key for existing nodes and uses an asymmetric key approach to share the pairwise keys for a new node after deployment. However, since the initial key *KI* is used to compute the individual keys and the pairwise keys after deployment for all nodes, if an adversary obtains *KI*, the adversary has the ability to compute all individual keys and the pairwise keys for all nodes.

On the other hand, Du et al. use a modular arithmetic-based symmetric key approach to share the pairwise key between a sensor node and a cluster head. Thus, a sensor node cannot directly establish a pairwise key with other sensor nodes and, instead, it requires the support of the cluster head. In their scheme, inorder to establish a pairwise key between two nodes in the same cluster, the cluster head randomly generates a pairwise key and encrypts it using the shared keys with these two nodes. Then the cluster head transmits the encrypted pairwise key to each node. Thus, if the cluster head is compromised,the pairwise keys between non-compromised sensor nodes in the same cluster will also be compromised.

- We show the security weaknesses of existing ECC based key management schemes for dynamic WSNs.
- We propose the first certificateless effective key management scheme (CL-EKM) for dynamic WSNs. CL-EKM supports four types of keys, each of which is used for a different purpose, including secure pair-wise node communication and group-oriented key communicationwithin clusters. Efficientkey management procedures are defined as supporting node movements across different clusters and key revocation process for compromised nodes.
- CL-EKM is implemented using Ubuntu OS and to measure the computation and communication overhead of CL-EKM. Also we develop a simulator to measure the energy consumption of CL-EKM.

OVERVIEW OF THE CERTIFICATELESS EFFECTIVE KEY MANAGEMENT SCHEME

In this paper, we propose a Certificateless Key Management scheme (CL-EKM) that supports the establishment of four types of keys, namely: a certificateless public/private key pair, an individual key, a pairwise key, and a cluster key. This scheme also utilizes the main algorithms of the CL-HSC scheme [13] in deriving certificateless public/private keys and pairwise keys. We briefly describe the major notations used in the paper (See Table I), the purpose of these keys and how they are setup.

3. PROPOSED MODELLING

A. Types of Keys

Certificateless Public/Private Key:

Before a node is deployed, the KGC at the BS generates a unique certificateless private/public key pair and installs the keys in the node. This key pair is used to generate a mutually authenticated pairwise key.

Individual Node Key:

Each node shares a unique individual key with BS. For example, a L-sensor can use the individual key to encrypt an alert message sent to the BS, or if it fails to communicate with the H-sensor. An H-sensor can use its individual key to encrypt the message corresponding to changes in the cluster. The BS can also use this key to encrypt any sensitive data, such as compromised node information or commands. Before a node is deployed, the BS assigns the node the individual key.

Pairwise Key:

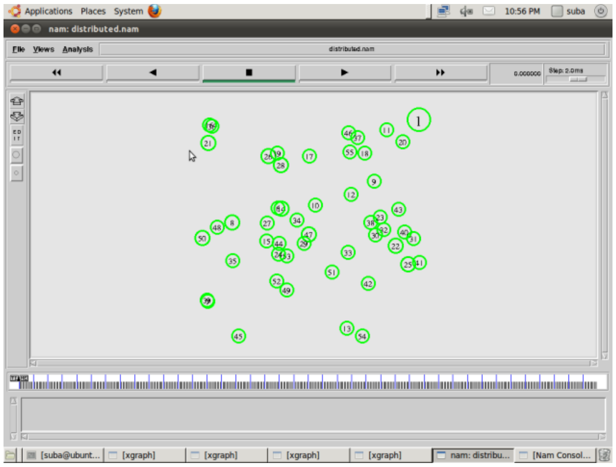
Each node shares a different pairwise key with each of its neighboring nodes for secure communications and authenticationof these nodes. For example, in order to join a cluster, a L-sensor should share a pairwise key with the H-sensor. Then, the H-sensor can securely encrypt and distribute its cluster key to the L-sensor by using the pairwise key. In an aggregation supportive WSN, the L-sensor can use its pairwise key to securely transmit the sensed data to the H-sensor. Each node can dynamically establish the pairwise key between itself and another node using their respective certificateless public/private key pairs.

Cluster Key:

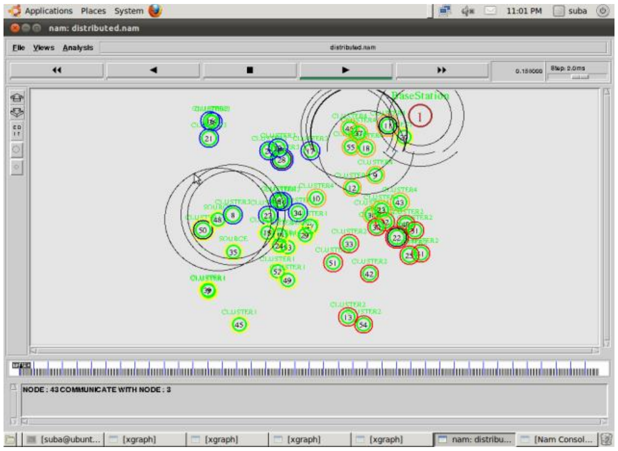
All nodes in a cluster share a key, named as cluster key. The cluster key is mainly used for securing broadcast messages in a cluster, e.g., sensitive commands or the change of member status in a cluster. Only the cluster head can update the cluster key when an L-sensor leaves or joins the cluster.

4. RESULTS AND DISCUSSION

Initialization of mobile node

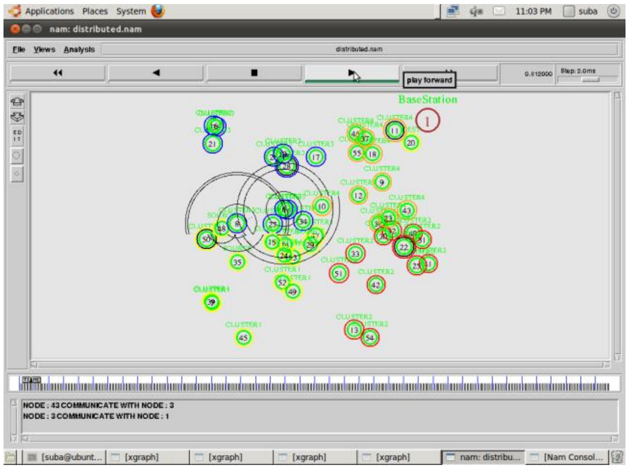

Applications Places System
10:56 PM
suba
nam: distributed.nam
File Views Analysis
distributed.nam
0.000000
Step: 2.0ms
[suba@ubunt... [xgraph] [xgraph] [xgraph] [xgraph] nam: distribu... [Nam Consol...

Base station communicate with cluster head



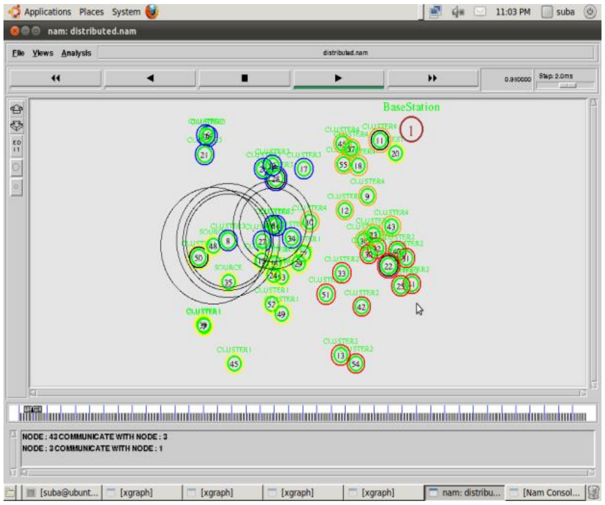
```
NODE : 43 COMMUNICATE WITH NODE : 3
```

Cluster head communicate with the node



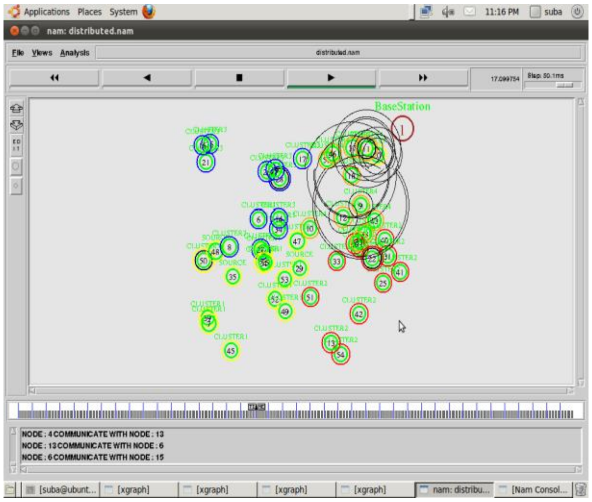
```
NODE : 43 COMMUNICATE WITH NODE : 3
NODE : 3 COMMUNICATE WITH NODE : 1
```

Cluster head communicate with the another cluster head



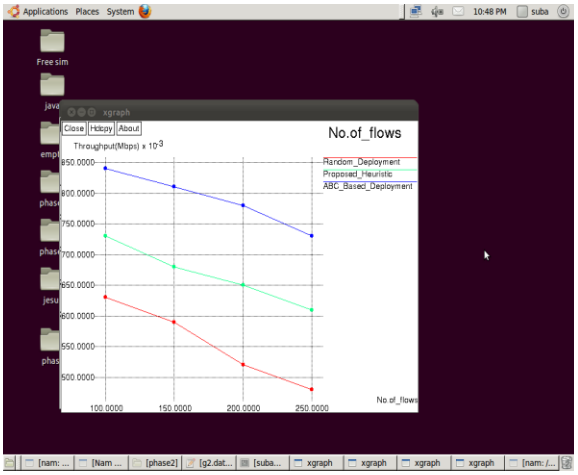
```
NODE : 43 COMMUNICATE WITH NODE : 3
NODE : 3COMMUNICATE WITH NODE : 1
```

Base station send the data through the public/private key pairs

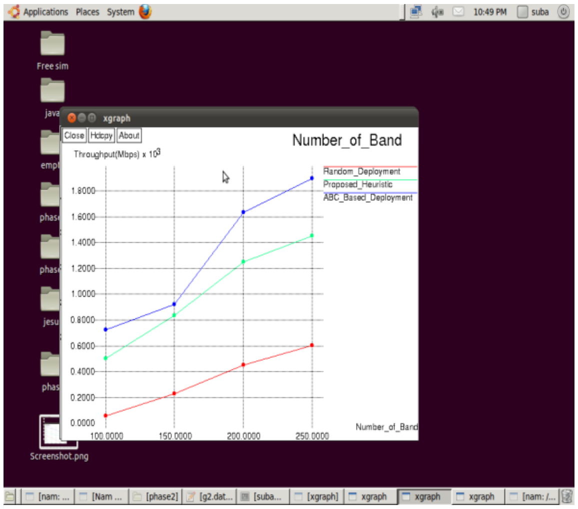


```
NODE : 4 COMMUNICATE WITH NODE : 13
NODE : 13 COMMUNICATE WITH NODE : 6
NODE : 6 COMMUNICATE WITH NODE : 15
```

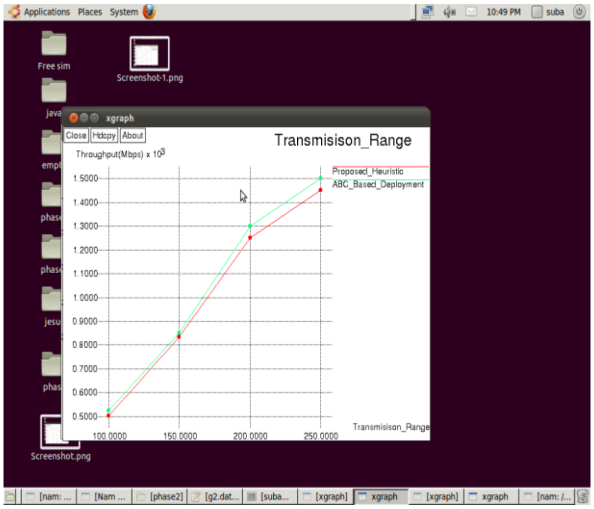
Data Flow graph



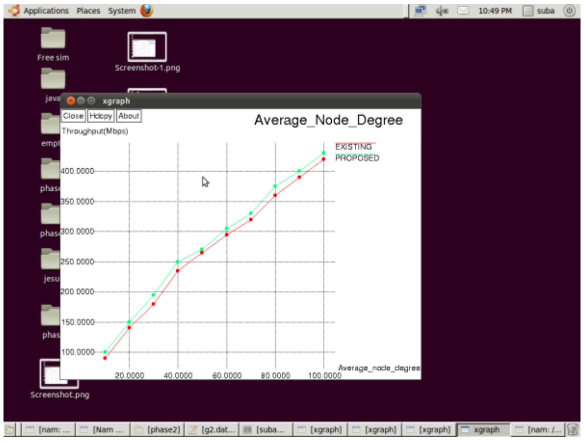
Number of Bandwidth



Transmission Range of data



Average Node data for communicate



5. CONCLUSION

In this paper, propose the first certificateless effective key management protocol (CL-EKM) for secure communicationin dynamic WSNs. CL-EKM supports efficient communication for key updates and management when a node leaves or joins a cluster and hence ensures forwardand backward key secrecy. Our scheme is resilient against node compromise, cloning and impersonation attacks and protects the data confidentiality and integrity. The experimental results demonstrate the efficiency of CL-EKM in resource constrained WSNs.

REFERENCES

[1] D. S. Sanchez and H. Baldus, "A deterministic pairwise key predistribution scheme for mobile sensor networks," in *Proc. 1st Int. Conf.SecureComm*, Sep. 2005, pp. 277–288.

[2] I.-H. Chuang, W.-T. Su, C.-Y. Wu, J.-P. Hsu, and Y.-H. Kuo, "Twolayered dynamic key management in mobile and long-lived clusterbased wireless sensor networks," in *Proc. IEEE WCNC*, Mar. 2007,pp. 4145–4150.

[3] S. Agrawal, R. Roman, M. L. Das, A. Mathuria, and J. Lopez, "A novel key update protocol in mobile sensor networks," in *Proc. 8th Int. Conf.ICISS*, vol. 7671. 2012, pp. 194–207.

[4] S. U. Khan, C. Pastrone, L. Lavagno, and M. A. Spirito, "An energy andmemory-efficient key management scheme for mobile heterogeneous sensor networks," in *Proc. 6th Int. Conf. CRiSIS*, Sep. 2011, pp. 1–8.

[5] X. Zhang, J. He, and Q. Wei, "EDDK: Energy-efficient distributed deterministic key management for wireless sensor networks," *EURASIPJ. Wireless Commun. Netw.*, vol. 2011, pp. 1–11, Jan. 2011.

[6] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," in *Proc. 6th Int.Workshop Cryptograph. Hardw. Embedded Syst.*, 2004, pp. 119–132.

[7] S. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proc. 9th Int. Conf. ASIACRYPT*, vol. 2894. 2013,pp. 452–473.

[8] S. Seo and E. Bertino, "Elliptic curve cryptography based certificatelesshybrid signcryption scheme without pairing," CERIAS, West Lafayette,

[9] IN, USA, Tech. Rep. CERIAS TR 2013-10, 2013. [Online]. Available:https://www.cerias.purdue.edu/apps/reports_and_papers/.Seu ng-Hyun

[10] D. Du, H. Xiong, and H. Wang, "An efficient key management scheme for wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2012, Sep. 2012, Art. ID 406254.