Group Communication based Key Establishment Scheme for Wireless Sensor Networks

Ashish H. Narvekar
Goa University
Computer Engineering Department
Goa College of Engineering Farmagudi-Goa
nh_ashish@yahoo.co.in

Nagaraj K. Vernekar
Goa University
Computer Engineering Department
Goa College of Engineering Farmagudi-Goa
nkv_2447@yahoo.com

ABSTRACT

Wireless sensor networks have been a hot topic of research over the past few years. They have been used by the military for border surveillance purposes and have since gained access into industrial and civilian uses such as weather, pollution, traffic control, and healthcare. One aspect of wireless sensor networks on which research has been conducted is the security of wireless sensor networks. Asymmetric key cryptography is widely used for the purpose of confidential key exchange and authentication. Wireless sensor networks (WSN) however are a class of devices with very low battery power and cannot use asymmetric key cryptography efficiently. This paper describes a scheme for hierarchical WSN which enables secure exchange of messages within clusters of sensor nodes using only symmetric key cryptography. The low battery power and very limited memory of the sensor nodes have been the main motivation for the proposed scheme which involves minimal number of computations, thus requiring less power for processing and less number of keys stored per sensor node, thus requiring less memory space.

General Terms

Wireless Sensor Networks, Cryptography

Keywords

Key establishment, Hierarchical wireless sensor networks, Base station, Cluster head, Sensor node, Cluster key.

1. INTRODUCTION

A wireless sensor network (WSN) [1] consists of distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, vibration, pressure and to cooperatively pass their data through the network to a main location The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, smart homes, etc.

The energy-constrained nature [2] of the sensor networks makes the task of incorporating security, a challenging problem. Most of the well-known security mechanisms introduce significant overhead and require a lot of computation and communication resources. Since the design of security protocols for sensor networks should be geared towards resource conservation, the level of security versus the consumption of energy, computations and memory resources constitute a design trade-off.

2. NETWORK SETTING

Key Management [3] is the most important issue in the security of Wireless Sensor Networks. It helps in maintaining the confidentiality of secret information from unauthorized users.

Architecture of Hierarchical WSN

In a Hierarchical WSN (HWSN) [4] there is a hierarchy among the nodes based on their capabilities: base station, cluster heads and sensor nodes. Base stations are many orders of magnitude more powerful than sensor nodes and cluster heads. A base station is typically a gateway to another network, a powerful data processing / storage center, and an access point for human interface. Base stations collect sensor readings; perform costly operations on behalf of sensor nodes and manage the network. Base stations are usually used as key distribution centers. Nodes with better resources, named as cluster heads are used to collect and merge local traffic and send it to base stations. Transmission power of a base station is usually enough to reach all sensor nodes, but sensor nodes have lower computation power and communication power. Thus, data flow in such networks can be: (i) pair-wise (unicast) among sensor nodes, (ii) group-wise (multicast) within a cluster of sensor nodes, and (iii) network-wise (broadcast) from base stations to sensor nodes.

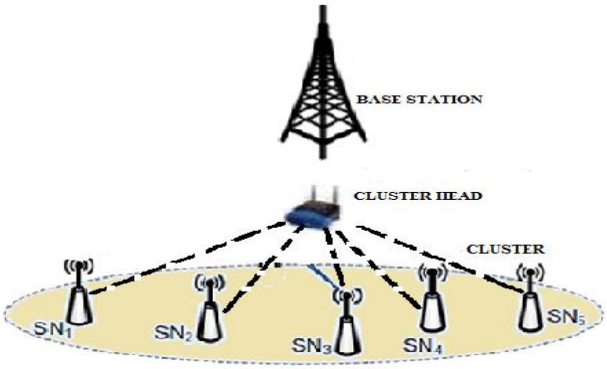


Fig. 1 System Architecture

3. ALGORITHM

Step 1: Pre-deployment Key Distribution

Load the sensor nodes with pair of keys (K_i , K_x).

K_i – Private keys generated by the base station as a set of relatively prime numbers.

K_x – Key to encrypt the X value obtained after solving the congruence system.

Step 2: Network Deployment
The sensor nodes are dispersed in the field of application.

Step 3: Clustering
The CH broadcasts a message. The sensor nodes within the close proximity of the CH respond to the message and thus form a cluster.

Step 4: Congruence System
The CH chooses a randomly generated cluster key CK and forms a congruence system as follows:
$X \equiv a_1 \pmod{K_1}$
$X \equiv a_2 \pmod{K_2}$
:
$X \equiv a_n \pmod{K_n}$
Where $a_i = CK \oplus K_i$ and K_i is the secret key of SN_i
CH solves the system of congruence equations to obtain the value of X.

Step 5: Encrypt X to form Y
$Y = (\text{Ones complement of } X) \oplus K_x$

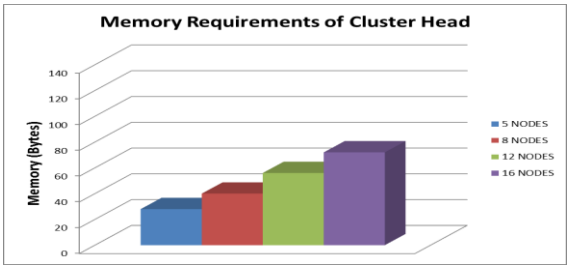
Step 6: Broadcast Y
The value Y is broadcasted by the CH within the cluster.

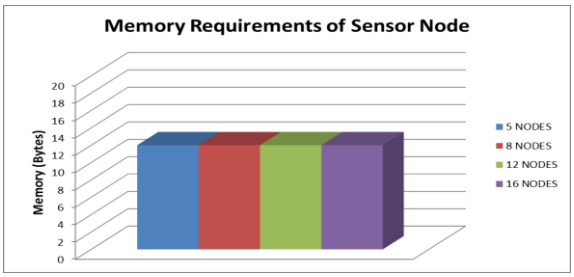
Step 7: Calculate CK at individual sensor node

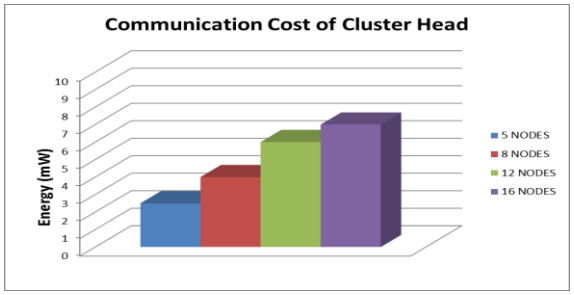
i. Extract the value of X as: $X = Y \oplus K_x$
X= Ones complement of X

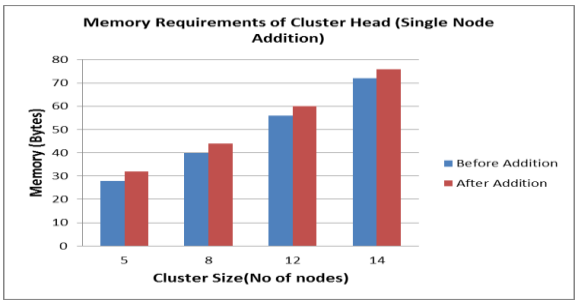
ii. Calculate CK as: $CK = (X \bmod K_i) \oplus K_i$

4. RESULTS









5. PERFORMANCE ANALYSIS

Memory Space Requirement
The CH would store one CK, one encryption key K_x and n private keys, where n is the number of sensor nodes in the cluster. The sensor node would store one private key, one CK, and one encryption key K_x.

Computation Requirement
The agent node generates a random cluster key and solves the congruence system in minimal time. Also it performs exclusive-or and one's complement. The sensor node would perform two exclusive-or, one one's complement and one mod operation. Thus the scheme involves reasonable number of computations.

6. CONCLUSION

The key establishment scheme has been proposed for a hierarchical WSN. It is based on the concept of group communication within a cluster consisting of a cluster head and sensor nodes. The scheme makes use of modular arithmetic for the key establishment process. It involves less number of computations and communication and thus requires less battery power. It also requires lower memory space as compared to the various schemes discussed in the literature. This scheme thus provides efficient means of key establishment in WSN.

7. REFERENCES

[1] Lin Shen and Xiangquan. A Dynamic Cluster-based Key Management Protocol in Wireless Sensor Networks- SHI, International Journal Of Intelligent Control And Systems, Vol. 13, No. 2, June 2008, 146-151

[2] Gaurav Jolly, Mustafa C. Kuşçu, Pallavi Kokate, and Mohamed Younis. A Low-Energy Key Management Protocol for Wireless Sensor Networks-, Computer Science and Electrical Engineering, University of Maryland, Baltimore County, Baltimore, Maryland

[3] Syed Muhammad Khaliq-ur-Rahman Raazi, Zeeshan Pervez and Sungyoung Lee. Key Management Schemes of Wireless Sensor Networks: A Survey-, Department of Computer Engineering, Kyung Hee University, Global Campus, Korea

[4] Önder KHALIL1, Suat OZDEMIR. Performance Evaluation Of Key Management Schemes In Wireless Sensor Networks, Gazi University, Computer Engineering Department, Maltepe Ankara