Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on Security and Energy Consumption While Transferring Data through Cluster Based Wireless Sensor Networks

Payal Machirkar, Nita Thakare, Animesh Tayal
Department of Computer Technology
PCE, Nagpur, India

Abstract*—Wireless sensor networks are ad-hoc networks comprised mainly of small sensor nodes with limited resources, and are rapidly emerging as a technology for large-scale, low- cost, automated sensing and monitoring of different environments of interest. Cluster-based communication has been proposed for these networks for various reasons such as scalability, low cost and energy efficiency. In this paper, we investigate the problem of adding security to cluster- based communication protocols for homogeneous wireless sensor networks consisting of sensor nodes with severely limited resources, and propose a security solution for the network, a protocol where clusters are formed dynamically and periodically. Here the security issue is concerned while transferring the data or information through cluster-based wireless sensor network. In this paper we have studied the different tools for the security purposes for transferring the data.

***Keywords*—ESPDA , NOVSF codes, SEEDR algorithm**

I. INTRODUCTION

A wireless sensor network (WSN) is a network system comprised of spatially distributed devices using wireless sensor nodes to monitor physical or environmental conditions, such as sound, temperature, and motion. The individual nodes are capable of sensing their environments, processing the information data locally, and sending data to one or more collection points in a WSN [1]. Efficient data transmission is one of the most important issues for WSNs. Meanwhile, many WSNs are deployed in harsh, neglected, and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings [2].

Cluster-based communication protocols have been proposed for ad hoc networks in general and sensor networks in particular for various reasons including scalability and energy efficiency. In cluster-based networks, nodes are organized into clusters, with cluster heads (CHs) relaying messages from ordinary nodes in the cluster to the BSs[3]. Adding security to WSNs is specially challenging. Existing solutions for conventional and even other wireless ad hoc networks are not applicable here, given the lack of resources in sensor nodes. Public-key-based methods are one such example. In addition, efficient solutions can be achieved only if tailored to particular network organizations. In this paper, we investigate the problem of adding security to cluster-based communication protocols for homogeneous WSNs (those in which all nodes in the network, except the BSs, have comparable capabilities).

II. RELATED WORK

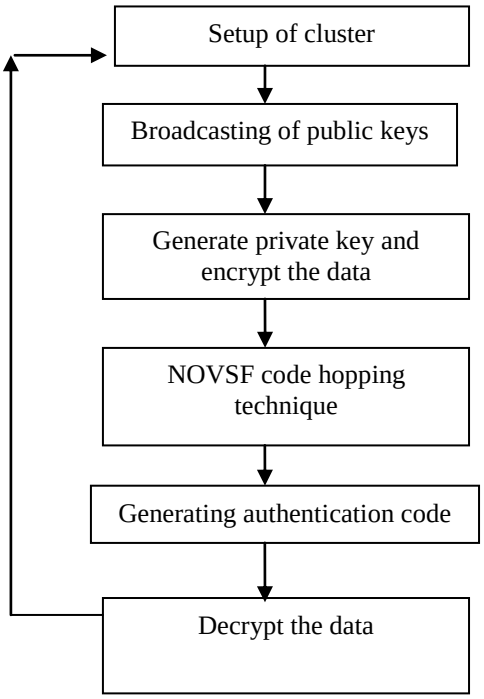
The number of literatures specifically targeted to security of WSNs has grown significantly. Here , we discuss about the studies based on cryptographic methods, and focus on those targeted to access control for WSN.

Adrian Carlos Ferreira et al.[3] focused on adding security to cluster-based communication protocols in homogeneous WSNs with resource-constrained sensor nodes. The author tells about the SLEACH, the first modified version of LEACH with cryptographic protection against outsider attacks. It prevents an intruder from becoming a CH or injecting bogus sensor data into the network. SLEACH is quite efficient, and preserves the structure of the original LEACH, including its ability to carry out data fusion. The simplicity of our solution relies on LEACH's assumption that every node can reach a BS by transmitting with sufficiently high power.

Zhou Ruyan, Chen Ming et al. introduces the the cluster-based routing protocols for wireless sensor network based on genetic clustering algorithm. In the network of non-uniform distribution nodes, this method can select the cluster heads after setting the nodes. During the operation of the WSN, when the geographic location change or failure of cluster heads, WSN need to be re-cluster or reselecting the cluster heads, the method proposed in the paper can be used. By using this method, the scientific and rational treatment results can be gotten, which has important practical ignificance in balancing the network energy and extending the network life cycle[4].

Vishnu Kumar et al. [5] proposed a cluster based sensor network consist hundreds of small sensor node, each node has the sensing ability with less computational and communication power. Even though Sensor node has a basic hardware and software for manipulating the given task This paper presents a secure energy efficient dynamic routing

scheme (SEEDR) for wireless sensor networks. SEEDR uses a symmetric cryptography algorithm to support security. The dynamic key exchange protocol based on DH (Diffie-Hellman) algorithm is proposed, with non-blocking OVSF codes. Conceptual process of the algorithm is illustrated in figure.1 (a). Attackers cannot decrypt the information unless the private key is known. Using the public key the attackers cannot generate the private key.



(a)

Figure 1. (a) Conceptual flow of the SEEDR algorithm

In this paper, authors mainly present the design of Secure-EED(secure energy efficient dynamic routing protocol). The core idea of our protocol is derived by using Diffie-Hellman algorithm with NOVSF code-Hopping technique which not only provides a variety of security features, but also increase the efficiency of the entire network in terms of energy. It has been proved by simple analysis that our algorithm needs communication cost,less storage and computation power which makes the network more stable and secured.

I-Hsun Chuang et al gaves the A resource-efficient key management protocol which was essential for security-sensitive applications in wireless sensor networks (WSN). Moreover, the dynamic pair-wise key and group key management protocols are also important for long-lived and mobile WSN. In this paper, a Two-layered Dynamic Key Management (TDKM) approach for cluster-based WSN (CWSN) is proposed. Both pair-wise key and group key are distributed in three rounds for key material exchange without encryption/decryption and exponentiation operations in TDKM. In theoretical analysis, TDKM is compared with other key management protocols to show its efficiency.

The performance of TDKM is analyzed and compared with other group key management protocols [6] in several performance metrics including rounds, computation overhead, number of messages, and message size. The notations used for performance comparison are listed as follows:

1. n: the number of GMs in the group,
2. i: the index of GM,
3. OH(): the complexity of hash operation,
4. ODec(): the complexity of decryption operation,
5. OEnc(): the complexity of encryption operation,
6. OExp(): the complexity of exponentiation operation,
7. OMul(): the complexity of multiplication operation,
8. ODiv(): the complexity of division operation.

This paper contains the the two-layered dynamic key management (TDKM) approach was proposed for cluster-based wireless sensor networks. In fact, this technique was easily applied to multi-level network architecture. By comparing TDKM with tree-based approaches, no encryption/decryption operation was required to transmit the materials of group key in TDKM. By comparing TDKM with contribution-based approaches, multiplication operation instead of exponentiation operation was used to generate group key. Moreover, the total round of group key generations is constant and the computational complexity is O(n2) for TDKM. Furthermore, the simplified TDKM was also proposed to enhance the system performance. For simplified TDKM, GL only needs to perform O(n) hash operations to transmit the materials of group key and each GM only needs to perform constant times of hash operations to generate the group key. Finally, the relationships between system performance and the number of groups are analyzed[6].

P. Nuir et al [7] presented an Energy-efficient and Secure Pattem-based Data Aggregation protocol (ESPDA) for wireless sensor networks. ESPDA was energy and bandwidth efficient because cluster-heads prevent the transmission of redundant data from sensor nodes. ESPDA was also secure because it does not require the encrypted data to be decrypted by cluster-heads to perform data aggregation. In ESPDA, cluster-head first requests sensor nodes to send the corresponding pattern code for the sensed data. If multiple sensor nodes send the same pattern code to the cluster-head, then only one of them is permitted to send the data to the cluster-head. Hence, ESPDA has advantages over the conventional data aggregation techniques with respect to energy, bandwidth efficiency and security. Simulations results show that as data redundancy increases, the amount of data transmitted from sensor nodes to cluster-head decreases up to 45% when compared to conventional algorithms.

This paper proposes an Energy-efficient and Secure Patten based Data Aggregation protocol (ESPDA) for cluster-based wireless sensor networks. Knowing that 70% of the energy consumption was due to data transmission [3], the proposed ESPDA reduces data transmission by not sending the redundant data from sensor nodes to cluster-heads. Since the number of sensors in a sensor network was very large, often various sensors detect common data. Data aggregation [4] is used to eliminate redundancy and minimize the number of transmissions in order to save energy. In conventional data aggregation methods, cluster-heads receive all the data from sensor nodes and then eliminate the redundancy by checking the contents of the data as shown in Figure l(b). In ESPDA, instead of transmitting the entire data with redundancy, the sensor nodes send the corresponding pattern codes to cluster-head for data aggregation. Thus, data aggregation is performed even before the actual data is transmitted from the sensor nodes as illustrated in Figure l(c).

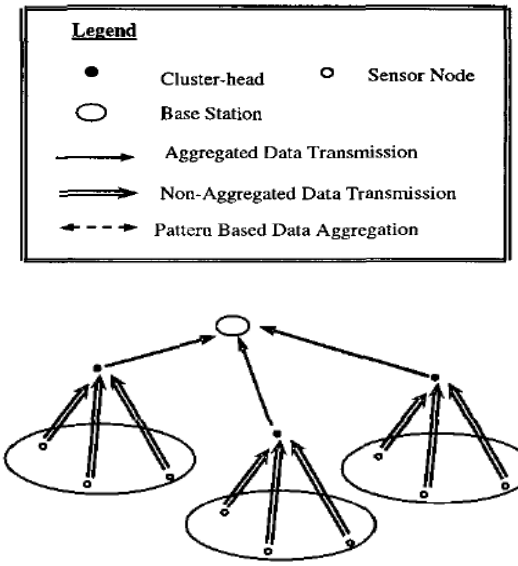


Figure l(b). Transmission of Data using conventional data aggregation.

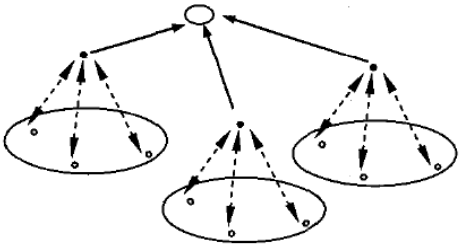


Figure I(c). Transmission of Data using ESPDA technique

This paper has introduced an energy-efficient and secured data aggregation protocol called ESPDA. In contrast to Conventional data aggregation protocols ESPDA avoids the transmission of redundant data from the sensor nodes to the cluster-head. To make the data transmission and aggregation more secured cluster-head is not required for decrypting or encrypting the data received from the sensor nodes. The symmetric keys which are used due to their low memory space and computing requirements, are not transmitted between the cluster-head and the sensor nodes. Simulation results show that ESPDA technique improves the energy and bandwidth efficiency and the protocol reduces the number of packets transmitted. Thus when ESPDA is integrated with our previously proposed security protocol it greatly helps to achieve the primary goal of energy efficiency and security essential in wireless sensor networks[7].

ACKNOWLEGEMENT

In this paper we studied the different techniques for secured data transmission using the clustered based wireless sensor network. Clustered based sensor network has been proposed for the ad-hoc network. In this study the idea getting for an efficient and secured transmission of data. So in the future work we will implement the network with an efficient time and space constraining algorithm.

REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of SecurityIssues in Wireless Sensor Networks," IEEE Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.

[3] Adrian Carlos Ferreira 1 , Marcos Aur´elio Vila¸ca 1 , Leonardo B. Oliveira 1 , Eduardo Habib 1 , Hao Chi Wong 1 , Antonio A.Loureiro 1,"On the Security of Cluster-based Communication Protocols for Wireless Sensor Networks", Federal University of Minas Gerais, MG,Brazil.

[4] Zhou Ruyan, Chen Ming, Feng Guofu, Liu Huifang, He Shijun,"Genetic Clustering Route Algorithm in WSN", 2010 Sixth International Conference on Natural Computation (ICNC 2010), 978-1-4244-5961-2/10/$26.00 ©2010 IEEE.

[5] Vishnu Kumar, Yunjung Park, Dugki Min, Eunmi Choi," Secure-EEDR: Dynamic key exchange protocol based on Diffie-Hellman algorithm with NOVSF code-hopping technique for wireless sensor networks", 2010 International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering .

[6] I-Hsun Chuang1, Wei-Tsung Su1, Chun-Yi Wu2, Jang-Pong Hsu2, Yau-Hwang Kuo1," Two-layered Dynamic Key Management in Mobile and Long-lived Cluster-based Wireless Sensor Networks", This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2007 proceedings, 1525-3511/07/$25.00 ©2007 IEEE.

[7] H. cum, S. Ozdemir, P. Nuir*, D. Muthuavinashiappun," ESPDA: ENERGY-EFFICIENT AND SECURE PATTERNBASED DATA AGGREGATION FOR WIRELESS SENSOR NETWORKS", 0-7803-813 3-5/03/$17.0002 003 IEEE.

