SECURE AND EFFICIENT DATA TRANSMISSION FOR CLUSTER-BASED WIRELESS SENSOR NETWORKS

Reddi.Bhargavi Naga Kumari, Sri.G.Ramesh Kumar, Sri.V.Bhaskara Murthy,
MCA Student, Assistant Professor, Associate Professor
Dept Of MCA
B.V.Raju College, Bhimavaram

ABSTRACT

Secure data transmission is a critical issue for wireless sensor networks (WSNs).Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. We propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while its security relies on the hardness of the discrete logarithm problem. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to] illustrate the efficiency of the proposed protocols. The results show that, the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

I. INTRODUCTION

Awireless 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. 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. Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs.

1.1 Background and Motivations

Cluster-based data transmission in WSNs, has been investigated by researchers in order to achieve the network scalability and management, which maximizes node lifetime and reduce bandwidth consumption by using local collaboration among sensor nodes. In a cluster-based WSN (CWSN), every cluster has a leader sensor node, regarded as cluster-head (CH). A CH aggregates the data collected by the leaf nodes (non- CH sensor nodes) in its cluster,

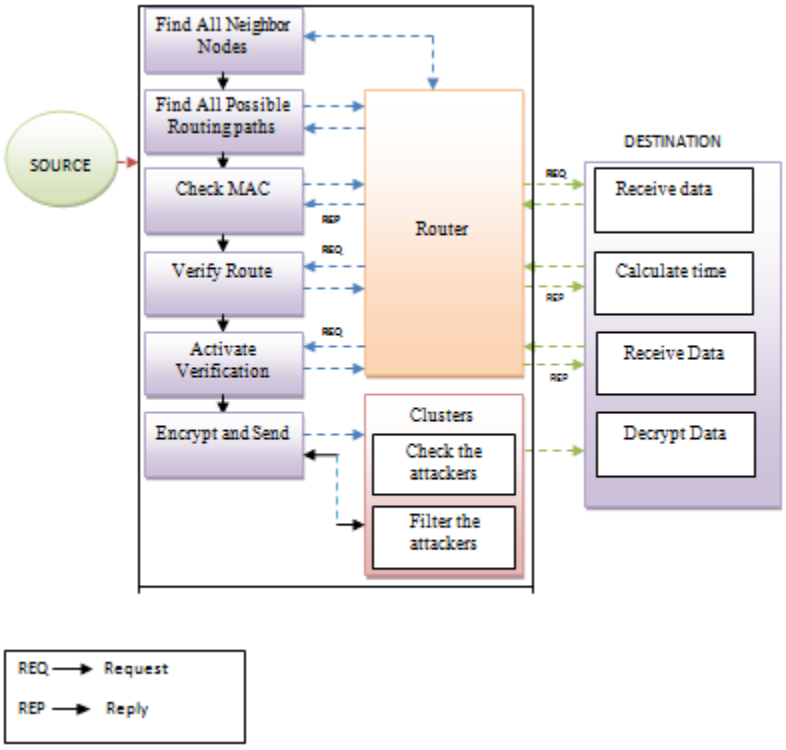
and sends the aggregation to the base station (BS). The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman *et al*. is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. In order to prevent quick energy consumption of the set of CHs, LEACH randomly rotates CHs among all sensor nodes in the network, in rounds. LEACH achieves improvements in terms of network lifetime. Following the idea of LEACH, a number of protocols have been presented such as APTEEN and PEACH, which use similar concepts of LEACH. In this paper, for convenience, we call this sort of cluster-based protocols as LEACH-like protocols. Researchers have been widely studying CWSNs in the last decade in the literature, however, the implementation of the cluster-based architecture in the real world is rather complicated.

Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links. Therefore, providing steady long-lasting node-to-node trust relationships and common key distributions are inadequate for LEACH-like protocols (most existing solutions are provided for distributed WSNs, but not for CWSNs). There are some secure data transmission protocols based on LEACH-like protocols, such as SecLEACH, GS-LEACH and RLEACH . Most of them, however, apply the symmetric key management for security, which suffers from a so-called orphan node problem. This problem occurs when a node does not share a pairwise key with others in its preloaded key ring, in order to mitigate the storage cost of symmetric keys, and the key ring is not sufficient for the node to share pairwise symmetric keys with all of the nodes in a network. In such a case, it cannot participate in any cluster, and therefore, has to elect itself as a CH. Furthermore, the orphan node problem reduces the possibility of a node joining a CH, when the number of alive nodes owning pairwise keys decreases after a longterm operation of the network. Since the more CHs elected by themselves, the more overall energy consumed of the network, the orphan node problem increases the overhead of transmission and system energy consumption by raising the number of CHs. Even in the case that a sensor node does share a pairwise key with a distant CH but not a nearby CH, it requires comparatively high energy to transmit data to the distant CH.

The feasibility of the asymmetric key management has been shown in WSNs recently, which compensates the shortage from applying the symmetric key management for security. Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate. The Identity-Based digital Signature (IBS) scheme, based on the difficulty of factoring integers from Identity-Based Cryptography (IBC), is to derive an entity's public key from its identity information, e.g., from its name or ID number. Recently, the concept of IBS has

been developed as a key management in WSNs for security. Carman first combined the benefits of IBS and key pre-distribution set into WSNs, and some papers appeared in recent years, e.g.. The IBOOS scheme has been proposed in order to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced by Even et al. The IBOOS scheme could be effective for the key management in WSNs. Specifically, the offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication. Some IBOOS schemes are designed for WSNs afterwards, such as and this system. The offline signature in these schemes, however, is precomputed by a third party and lacks reusability, thus they are not suitable for CWSNs.

II. SYSTEM ARCHITECTURE



III. EXISTING SYSTEM

In this Existing System of wireless sensor network 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.

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 .

IV. PROPOSED SYSTEM

In this Proposed System, Secure and efficient data transmission is thus especially necessary and is demanded in many such practical WSNs. So, we propose two Secure and Efficient data Transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively.

It has been proposed in order to reduce the computation and storage costs to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.

In the proposed protocols pairing parameters are distributed and preloaded in all sensor nodes by the BS initially.

V. IMPLEMENTATION

SET Protocol

In this module, Secure and Efficient data Transmission (SET) protocol for CWSNs. The SET-IBOOS protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The proposed SET-IBOOS operates similarly to the previous SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization, then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

Key management for security

In this module, security is based on the DLP in the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The IBOOS scheme in the proposed SET-IBOOS consists of following four operations, extraction, offline signing, online signing and verifications.

Key management

In this Module, the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security.

• Neighborhood authentication

In this module, used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Here, “limited” means the probability of neighborhood authentication, where only the nodes with the shared pairwise key can authenticate each other.

Storage cost

In this module, represents the requirement of the security keys stored in sensor node’s memory.

Network scalability

In this module, indicates whether a security protocol is able to scale without compromising the security requirements. Here, “comparative low” means that, compared with SET-IBS and SET-IBOOS, in the secure data transmission with a symmetric key management, the larger network scale increases, the more orphan nodes appear in the network.

Communication overhead

In this module, the security overhead in the data packets during communication. •

Computational overhead

In this module, the energy cost and computation efficiency on the generation and verifications of the certificates or signatures for security.

Attack resilience

In this module, the types of attacks that security protocol can protect against.

VI. CONCLUSION

In this paper, we first reviewed the data transmission issues and the security issues in CWSNs. The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols respectively for CWSNs, SET-IBS and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based crypto-system, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. Lastly, the comparison in the calculation and simulation results show that, the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, we pointed out the merits that, using SET-IBOOS with less auxiliary security overhead is preferred for secure data transmission in CWSNs.

Bibliography

Core Java™ 2 Volume I – Fundamentals 7th Edition

Pearson Education – Sun Microsystems

Core Java™ 2 Volume II – Advanced

Pearson Education – Sun Microsystems

Effective Java – Programming Language Guide

Pearson Education – Sun Microsystems

Java Swing – Covers Java2 SDK 1.4 2nd Edition

O'Reilly – SPD

Java Network Programming – First Edition

O'Reilly - SPD