Protected and Effective Data Communication for Cluster-Based Wireless Sensor Networks

GADDAM SRINIVAS
Department of Computer Science & Engineering (M. Tech)
Sindura College of Engineering and Technology
Ramagundam,Telangana

G.LAKSHMI
Asst. Professor,
Department of Computer Science (M. Tech)
Sindura College of Engineering and Technology
Ramagundam,Telangana

K.GEETA
Head of the Department of Computer Science
Sindura College of Engineering and Technology
Ramagundam,Telangana

Abstract:
Reliable data transmission is a critical issue for wireless sensor networks. Reliable means providing security for data transmission and providing efficiency in data transmission for cluster based wireless sensor networks. Clustering is an effective and practical way to enhance the system performance of wireless sensor networks. In this, the clusters are formed dynamically and periodically. The Identity based digital signature protocol is introduced in order to provide reliable data transmission for cluster-based wireless sensor networks. The Identity based digital signature protocol relies on the hardness of the Diffie-Hellman problem to provide security and also it reduces the computational overhead of the protocol using discrete logarithm problem. This paper includes the feasibility of the protocol with respect to security requirements and security analysis over several attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocol. The results show that, the proposed protocol have better performance than the existing secure protocols for cluster-based wireless sensor networks, in terms of security overhead and energy consumption.

Keywords: *Cluster-based wireless sensor networks, ID based digital signature, Reliable data transmission protocol*

1. Introduction

Wireless sensor network 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 wireless sensor network. Reliable data transmission is one of the most important issues for wireless sensor networks. Meanwhile, many wireless sensor networks are deployed in harsh, neglected and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings. Reliable data transmission is thus especially necessary and is demanded in many such practical wireless sensor networks.

2. Literature Survey

In a cluster-based wireless sensor network, every cluster has a leader sensor node, regarded as cluster-

head. A cluster-head aggregates the data collected by the leaf nodes (sensor nodes) in its cluster, and sends the aggregation to the base station. The Low-Energy Adaptive Clustering Hierarchy protocols a widely known and effective one to reduce and balance the total energy consumption for cluster based wireless sensor networks. In order to prevent quick energy consumption of the set of cluster-heads, Low-Energy Adaptive Clustering Hierarchy protocol randomly rotates cluster-heads among all sensor nodes in the network, in rounds. Adding security to Low-Energy Adaptive Clustering Hierarchy protocol is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links.

Furthermore, the orphan node problem reduces the possibility of a node joining a cluster-head, when the number of alive nodes owning pair wise keys decreases after a long term operation of the network. Since the more cluster-heads 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 cluster-heads. Even in the case that a sensor node does share a pair wise key with a distant cluster-head but not a nearby cluster-head, it requires comparatively high energy to transmit data to the distant cluster-head. 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 scheme, based on the difficulty of factoring integers from Identity-

Based Cryptography, is to derive an entity's public key from its identity information, e.g., from its name or ID number. Recently, the concept of Identity-Based digital Signature has been developed as a key management in wireless sensor networks for security. Carman first combined the benefits of Identity-Based digital Signature and key pre-distribution set into wireless sensor networks, and some papers appeared in recent years.

3. Proposed System Description

Consider a cluster-based wireless sensor network consisting of a fixed base station and a large number of wireless sensor nodes, which are homogeneous in functionalities and capabilities. It is assumed that the base station is always reliable, i.e., the base station is a trusted authority. Meanwhile, the sensor nodes may be compromised by attackers, and the data transmission may be interrupted from attacks on wireless channel. In a cluster-based wireless sensor network, sensor nodes are grouped into clusters and each cluster has a cluster-head sensor node, which is elected autonomously. Leaf sensor nodes, join a cluster depending on the receiving signal strength and transmit the sensed data to the base station via cluster-heads to save energy. The cluster-heads perform data fusion, and transmit data to the base station directly with comparatively high energy. In addition, it is assumed that, all sensor nodes and the base station are time synchronized with symmetric radio channels, nodes are distributed randomly, and their energy is constrained. In cluster-based wireless sensor networks, data sensing, processing and transmission consume energy of sensor nodes. The cost of data transmission is much more expensive than that of data processing. Thus, the method that the intermediate node (e.g., a cluster-head) aggregates data and sends it to the base station is preferred, than the method that each sensor node directly sends data to the base station. A sensor node switches into sleep mode for energy saving when it does not sense or transmit data, depending on the TDMA (time division multiple access) control used for data transmission. In this paper, the proposed Reliable Data Transmission Identity Based Digital Signature Protocol is designed for the same scenarios of cluster-based wireless sensor networks.

4. Proposed Protocol

A. Objectives

The data transmission protocols for wireless sensor networks, including cluster based protocols, are vulnerable to a number of security attacks. Especially, attacks to cluster-heads in cluster-based wireless sensor networks could result in serious damage to the network, because data transmission and data aggregation depend on the cluster-heads fundamentally. If an attacker manages to compromise or pretend to be a cluster-head, it can provoke attacks such as sinkhole and selective forwarding attacks, hence disrupting the network. On the other hand, an attacker may intend to inject bogus sensing data into the wireless sensor network, e.g., pretend as a leaf node sending bogus information towards the cluster-heads. Nevertheless, Low-Energy Adaptive Clustering Hierarchy protocols are more robust against insider attacks than other types of protocols in wireless sensor networks. It is because cluster-heads are rotating from nodes to nodes in the network by rounds, which makes it harder for intruders to identify the routing elements as the intermediary nodes and attack them. The characteristics in Low-Energy Adaptive Clustering Hierarchy protocols reduce the risks of being attacked on intermediary nodes, and make it harder for an adversary to identify and compromise important nodes. The goal of the proposed reliable data transmission for cluster-based wireless sensor network s is to guarantee a secure and efficient data transmission between leaf nodes and cluster heads, as well as transmission between cluster heads and the base station. Meanwhile, most of existing secure transmission protocols for cluster-based wireless sensor networks in the literature, however, applies the symmetric key management for security, which suffers from the orphan node problem. The aim is to solve this orphan node problem by using the ID-based crypto-system that guarantees security requirements, and propose Reliable Data Transmission Identity Based Digital Signature Protocol by using the Identity Based Digital Signature scheme.

B.Methodologies

- Reliable Data Transmission Identity Based Digital Signature Protocol has been introduced. The key idea is 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 protocol, secret keys and pairing parameters are distributed and preloaded in all sensor nodes by the base station initially, which overcomes the key escrow problem described in Identity-based crypto-systems.
- Secure communication in Reliable Data Transmission Identity Based Digital Signature Protocol relies on the Identity-based cryptography, in which, user public keys are their Identity information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy.
- It shows the feasibility of the proposed protocols with respect to the security requirements and analysis against three attack models. Moreover, it compares the proposed protocols with the existing secure protocols for efficiency by calculations and simulations respectively, with respect to both computation and communication.

5. Protocol Operation

At the beginning the clusters are formed. The clusters are formed based on the cluster formation algorithm which takes location of the sensor nodes, distance from the base station and the energy of the sensor nodes as its parameters. After the cluster formation the cluster is head elected dynamically in each clusters. In a cluster, energy levels of each sensor nodes are compared with some threshold and cluster heads are selected accordingly. The base station then broadcasts its information to all cluster heads. The information includes ID of the base station, time stamp and nonce. The cluster head broadcasts its information to its sensor nodes. The information includes ID, time stamp, advertisement message, and digital signature. After receiving the information from cluster head, the sensor nodes join the cluster. The cluster head then broadcasts the scheduled message to its sensor

nodes. The sensor nodes transmit the sensed data to its cluster head. The cluster head aggregates the sensed data from its sensor nodes. The cluster head then transmits aggregated data to the base station.

6. Security Analysis

The proposed protocol is designed to resist against several types of attacks. The attacks are detected and the attacker node is thrown out off the network. The main goal of proposed protocol is to resist attacks such as passive attacks, flooding attacks and node compromising attack. Since the protocol is designed using polymorphic encryption methods which deals with passive attacks, the protocol is able to resist against passive attacks. The flooding attack can be resisted by the protocol. Since the protocol uses digital signature methods to authenticate the sensor nodes, the flooding can be detected by comparing the digital signatures and the attacker node is thrown out off the network. The node compromising attack is detected by the protocol. Since the protocol uses different time stamps for different rounds of communication. The protocol compares time stamps of all the nodes and if it finds different time stamp then that node is reported as attacker node and it is thrown out off the network. Hence the proposed protocol provides resistance against several types of attacks.

7. Conclusion

In this paper, it is reviewed that the data transmission issues and the security issues in cluster based wireless networks. The deficiency of the symmetric key management for secure data transmission has been discussed. It is then presented two secure and efficient data transmission protocols respectively for cluster based wireless networks, reliable data transmission identity based digital signature protocol. In the evaluation section, it is provided feasibility of the proposed reliable data transmission identity based digital signature protocol with respect to the security requirements and analysis against routing attacks. reliable data transmission identity based digital signature protocol is efficient in communication and applying the ID-based crypto-system, which achieves security requirements in cluster based wireless networks, 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 reliable data transmission identity based digital signature protocol has better performance than existing secure protocols for cluster based wireless networks.

References

1. A. Abbasi and M. Younis, “A survey on clustering algorithms for wireless sensor networks,” Comput. Commun., vol. 30, no. 14-15, 2007.
2. IEEE Trans. Wireless Commun., vol. 1, no. 4, 2002.
3. Manjeshwar, Q.-A.Zeng, and D. P. Agrawal, “An analytical model for information retrieval in wireless sensor networks using enhanced APTEEN protocol,” IEEE Trans. Parallel Distrib. Syst., vol.13, 2002
4. T. Hara, V. I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Info. Explosion Era, Stud. Comput. Intell. Springer-Verlag, 2010, vol. 278.
5. W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, application-specific protocol architecture for wireless microsensor networks,”
6. Y.Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks,” IEEE Commun. Surveys Tuts., vol. 8, no. 2, 2006.