International Journal on Applications in Engineering and Technology
Volume 2: Issue 1: January 2016, pp 20-30 www.aetsjournal.com ISSN (Online) : 2455-0523

ENERGY EFFICIENCY AND KEY BASED APPROACH FOR FORWARDING AGGREGATED DATA IN WIRELESS SENSOR NETWORKS

#Priyanka .R, ReshmaReghunath,Roshni .G, Vaishali .K, *S.Pathur Nisha

 # UG Scholar, *Professor, Dept. of CSE, Nehru Inst. of Tech, Coimbatore.

ABSTRACT

Energy cost of transmitting a single bit of information is approximately the same as that needed for processing a thousand operations in a typical sensor node. Thus, a practical way to prolong a wireless sensor network lifetime is to reduce the sensor energy consumption in data transmissions. Data aggregation is an efficient way to minimize energy consumption on sensors. In the proposed system, Sensor-Secure Data Aggregation scheme is used with the combination ofHomomorphic Encryption, Identity-Based Signature and Batch verification with an algorithm for filtering injected false data. The Homomorphic Encryption scheme provides a solution to secure data aggregation which makes it possible to aggregate n cipher texts into a single ciphertext without using any secret keys preserving fundamental arithmetic operations withconfidentiality.

Key words: Batch verification, Homomorphic encryption, identity-based signature, Secure data aggregation.

INTRODUCTION

Due to a need for robustness of monitoring and low cost of the nodes, wireless sensor networks (WSNs) are usually redundant. Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the computingpowerand

energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks. This cannot be remedied by cryptographic methods, because the attackers generally gain complete access to information stored in the compromised nodes. For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes. Thus, better, more sophisticated algorithms are needed for data aggregation in the future Wireless sensor networks. Such an algorithm should have two features.

1. In the presence of stochastic errors such algorithm should produce estimates which are close to the optimal ones in information theoretic sense. Thus, for example, if the noise present in each sensor is a Gaussian independently distributed noise with zero mean, then the estimate produced by such an algorithm should have a variance close to the Cramer- Rao lower bound (CRLB), i.e, it should be close to the variance of the Maximum Likelihood Estimator (MLE). However, such estimation should be achieved without supplying to the algorithm the variances of the sensors, unavailable in practice.

2. The algorithm should also be robust in the presence of non-stochastic errors such as faults and malicious attacks, and, besides aggregating data, such algorithm should also provide an assessment of the reliability and trustworthiness of the data received from each sensor node.

EXISTING SYSTEM

Due to limited computational power and energy resources, aggregation of data from multiple sensor nodes done at the aggregating node is usually accomplished by simple methods such as averaging. However such aggregation is known to be highly vulnerable to node compromising attacks. Since Wireless

Sensor Network are usually unattended and without tamper resistant hardware, they are highly susceptible to such attacks.Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the computingpower and energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging. However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks.

Disadvantages:

- Although the existing Iterative Filtering algorithms consider simple cheating behavior by adversaries, none of them take into account sophisticated malicious scenarios such as collusion attacks.
- If the node is compromised, then the attacker gain complete access to information stored in the compromised nodes.

PROPOSED SYSTEM

A new sophisticated collusion attack scenario against a number of existing Iterative filtering algorithms based on the false data injection is proposed. In such an attack scenario, colluders attempt to skew the aggregate value by forcing such Iterative Filtering algorithms to converge to skewed values provided by one of the attackers. A solution for vulnerability by providing an initial trust estimate which is based on a robust estimation of errors of individual sensors is proposed. Identification of a new sophisticated collusion attack against based reputation systems which reveals a severe vulnerability of Iterative Filteringalgorithms. A novel method for estimation of sensor's errors which is effective in a wide range of sensor faults and not susceptible to the described attack. Design of an efficient and robust aggregation method inspired by the MLE,

which utilizes an estimate of the noise parameters, obtained using contribution above. Enhanced Iterative filtering schemes able to protect against sophisticated collusion attacks by providing an initial estimate of trustworthiness of sensors using inputs from contributions.

SYSTEM ARHIECTURE

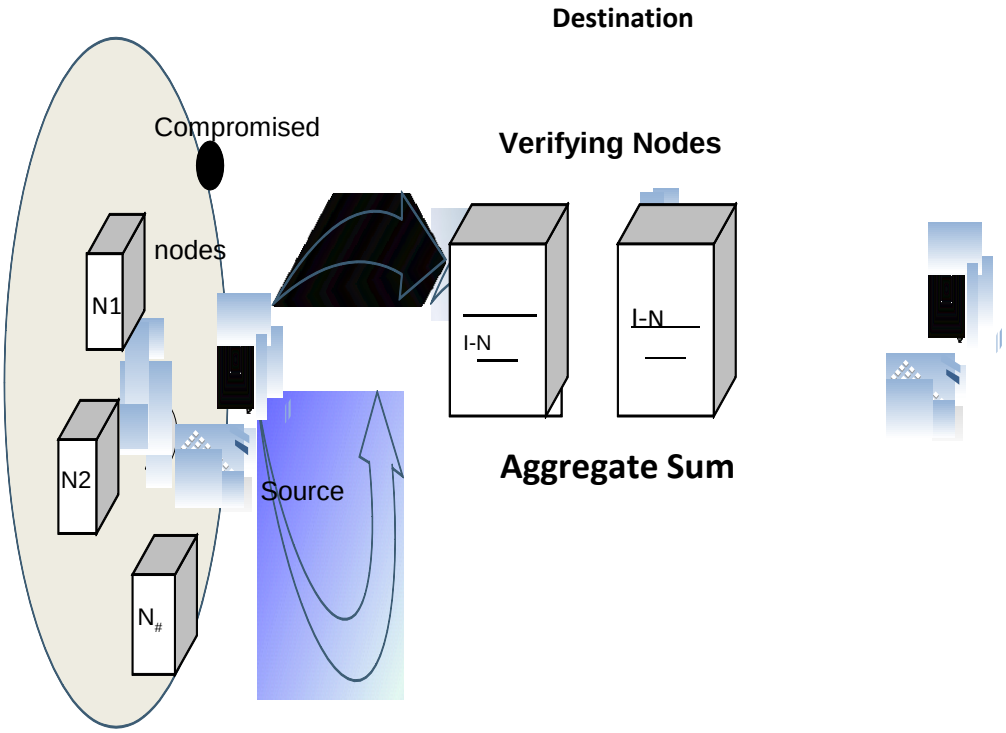

Fig no.1: System Architecture

N- Nodes, I-N-Intermediate nodes

In the Fig no.1, sensor nodes N are created which is taken as the source. The data from the source is send to the destination through the Intermediate nodes which is also called member nodes. The aggregate value will be send to the destination. The source node is also called as cluster heads. Compromised nodes will transfer the data and check whether the node is compromised node or not, then

it will transfer the data to the destination. The following sections are used to explain the proposed system in detail.

- Creation of nodes
- Homomorphic Encryption
- Batch Verification
- Intermediate Nodes
- Base Station

CREATION OF NODES

Initially the source nodes, intermediate nodes and destination node are created. Randomly one node act like Resource-head which get the data from other nodes and send the data to Recipient through verifying nodes. Small nodes are organized into Resources. In each Resource, one node is randomly selected as the Resource-head. To balance energy consumption, all nodes within a Resource take turns to serve as the Resource-head. That means physically there is no difference between a Resource-head and a normal node because the Resource-head performs the same sensing job as the normal node.

HOMOMORPHIC ENCRYPTION

Homomorphic Encryption makes it possible to aggregate n cipher texts into a single ciphertext without using any secret keys preserving fundamental arithmetic operations with confidentiality. After the node initialization the data will be encrypted and symmetric key is generated.

BATCH VERIFICATION

Batch verification techniques can reduce verification costs for multiple signatures. The proposed scheme supports fast multiple signature verification at the cluster heads by applying Binary Quick Search to the Batch verification for filtering injecting false data.

INTERMEDIATE NODES

Intermediatenodes are also called verifying nodes which are created during the node initialization. The key generated by the initial source node will be send to the intermediate node. The key received by the intermediate node will be compared with key that is send by the initial node. If the key is matching, it will be send to the next intermediate node. If it mismatches, immediately it identifies the injected sensor node.

BASE STATION

The Base station performs the verifications of signatures on cipher texts received from n clusters, and the decryption of the cipher texts. One type is called false report injection attacks, in which adversaries inject into networks the false data reports containing nonexistent events or faked readings from compromised nodes. These attacks not only cause false alarms at the Recipient. Resource (cluster head) node which get the data from other nodes and send the data to Recipient through Intermediate nodes.So the receiver can retrieve the complete original data by verifying the transmission at each node using homomorphic hash function.

ADVANTAGES OF PROPOSEDSYSTEM

- Provides a thorough empirical evaluation of effectiveness and efficiency.

- The results show that the proposed method provides both higher accuracy and better collusion resistance than the existing methods.
- Through the detail literature study, no existing work addresses on false data injection for a number of simple attack scenarios, in the case of a collusion attack by compromised nodes in a manner which employs high level knowledge about data.

RESULTS

Fig 1 Creation of Node

Fig2 Sensor Node1

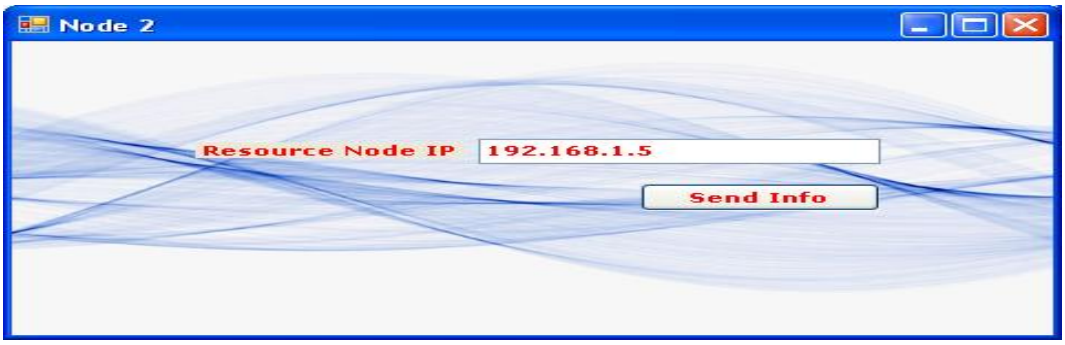

Fig 3 Sensor Node2

Fig.4 Resource

Fig.5 Report

Fig.6 Encrypted Report

CONCLUSIONS

Cryptographic primitives are fundamental building blocks for security protocols. It is not too much to say that the selection and integration of appropriate cryptographic primitives into the security schemes determines the efficiency and energy conservation of the whole scheme. This scheme shows how to integrate a set of the cryptographic primitives into a Secure Data Aggregation scheme in Homogeneous Sensor Networks to achieve security requirements. A practicalSecure Data Aggregation scheme based on the combination of the Homomorphic Encryption scheme, pairing-free Identity Based Scheme and the batch verification with Binary Quick Search for finding invalid signatures in heterogeneous clustered Wireless Sensor Networks . Sensor Secure Data Aggregation provides end-to-end confidentiality and hop-by-hop authentication. It determined the size of a cluster depending the ratio of the number of invalid signatures to minimize the efficiency of Cluster Head's batch verifications.

REFERENCES

1. Amin.F, Jahangir.A.H, and Rasifard.H, (2008), ”Analysis of Public Key Cryptography for Wireless Sensor Networks Security”, International Journal of Computer,Electrical andAutomobile Engineering

2. Bhavin N Patel, NehaPandya, (2013),“Secure Data Transfer using Cryptography With Virtual Energy for WSN”, International Journal of Engineering Trends and Technology (IJETT) – Vol. 04,Issue 08.

3. Gurjot Singh, SandeepKaurDhanda, (2014),” Quality of Service Enhancement of Wireless Sensor Network Using Symmetric Key Cryptographic Schemes”, I.J. Information Technology and Computer Science,Vol. 08, pp. 32-42

4. KarthikSenthilKumar.C, Sugumar.R, Nageshwari, (2013), ”Sensor Lifetime Enhancement Technique in WSN”, International journal of Computer Science and Information Technology,Vol. 3, No. 02.

5. KeyurParmar, Devesh C. Jinwala, (2015), ”Symmetric Key Based Homomorphic primitives for End to End Secure Data Aggregation”, Journal of Information Security, Vol. 06, pp. 38-50.

6. Krishnan.C, Malathy.G, (2014),”Data Aggregation Using RSA Key Management Technique in Wireless Sensor Networks”, International Journal of Innovative Research in Science, Engineering and Technology, Vol. 03, Issue 01.

7. RayalaUpendarRao(2012), ”Secure Routing in Cluster based Wireless Sensor Networks using Symmetric Cryptography with Session Keys”, International Journal of Computer Applications, Vol. 55 – 07.

8. SangeethaPatil, PadmapriyaPatil,(2014), ”Designing A Model for Energy Efficient and Secured Data Communication Using RSA algorithm WSN”, International Journal of Science And Research(IJSR), Vol. 03, Issue7.

9. SathyaRekha.U, Hemalatha.P, (2014),”Aggregating Multiple Applications in WSN Based On Symmetric Keys”,International Journal of Innovative Research in Science, Engineering and Technology, Vol. 03, Issue 03.

10. Suraj Kumar Khuraijam, Radhika.K.R(2013),”A Novel Symmetric Key Encryption Algorithm Based on RC5 in WSN”,International Journal of Emerging Technology and Advanced Engineering, Vol. 03, Issue 06.